Online Safety Policy

Perins School

2023-24

Approved by The Perins MAT Trust Board May 2023

Next review due May 2024

Contents

Contents ... 1

Development/Monitoring/Review of this Policy ... 3

Roles and Responsibilities ... 4

Policy Statements ... 6

Mobile Technologies Policy (inc. BYOD/BYOT) ... 8

Communications ... 12

Dealing with unsuitable/inappropriate activities ... 15

Responding to incidents of misuse ... 16

Illegal Incidents ... 17

Other Incidents ... 18

School actions & sanctions ... 18

Appendix ... 20

Student Acceptable Use Agreement ... 21

Parent/Carer Acceptable Use Agreement ... 22

Staff (and Volunteer) Acceptable Use Policy Agreement ... 23

Responding to incidents of misuse – flow chart ... 26

Record of reviewing devices/internet sites (responding to incidents of misuse) – Form online ... 27

Reporting Log (Online List) ... 28

Training Needs Audit Log (in conjunction with CPD lead) ... 29

School Technical Security Policy (including filtering and passwords) ... 30

School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (updated with new DfE guidance – September 2022) ... 44

Screening ... 46

School Online Safety Policy – Harmful Sexual Behaviour ... 47

Legislative background and context ... 47

Online ... 48

Policy for Harmful Sexual Behaviour ... 48

Related policies ... 48

Definitions ... 48

What is sexual violence? ... 49

What is sexual harassment? ... 49

Responsibilities ... 49

Leaders and DSLs ... 49

Staff ... 50

Governors ... 50

Learners ... 50

Parents/carers ... 50

Vulnerable groups ... 50

Reporting ... 51

Responding to an incident or disclosure ... 51

Risk assessment 51
Education 51
Training 52
Links 52
Social Media Policy Template 54
Online Safety Group Terms of Reference 60
Legislation 61
Links to other organisations or documents 65
Glossary of Terms 68
Audit of DfE identified areas for teaching in schools 68

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Safeguarding Lead
- Online Safety coordinator
- Staff – including teachers, support staff, technical staff.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	
The implementation of this online safety policy will be monitored by the:	Online safety coordinator: Lex Western (DSL) Data protection officer: Phil Segal
Monitoring will take place at regular intervals:	Twice a year (April & October)
The Students Standards Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Twice per year (in response to the monitoring)
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	October 2024
Should serious online safety incidents take place, the following external persons/agencies will be informed where appropriate:	Police Children's Services (via MASH) LADO

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) and filtering
- Internal monitoring data for network activity
- Device monitoring in lessons (Impero)
- Curriculum analysis (online safety education)
- Surveys/questionnaires of
  - students
  - parents/carers
  - staff

Scope of the Policy

This policy applies to all members of the Perins school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both inside and outside of the school premises.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Perins School.

Role of Trustees

The board of trustees are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding Trustee receiving regular information about online safety incidents and monitoring reports. The Safeguarding trustee has taken on the role of Online Safety trustee. The role of the Online Safety trustee will include:

- regular meetings with the Online Safety Coordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Board meeting

Headteacher and Senior Leaders

- The Executive Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Head of School and Online Safety Lead.
- The Executive Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.[i]
- The Executive Headteacher, Head of School and Senior Leaders are responsible for ensuring that the Online Safety Lead, Digital Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Executive Headteacher, Head of School and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.[ii]
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead and Digital Lead.

Online Safety Lead

- leads the Online Safety Group[iii]
- takes day to day responsibility for online safety issues.
- liaises with the Digital Lead and school technical staff.
- receives reports of online safety incidents and maintains a log of incidents to inform future online safety developments. Ensures CPOMS is updated as necessary.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- liaises with the Trustees.
- meets regularly with the Digital Lead and responsible Trustee to discuss current issues, review incident logs and filtering and change control logs.
- reports regularly to Senior Leadership Team.

Digital Lead

- has a leading role in establishing and reviewing the school online safety policies and documents.
- leads on training and advice for staff.
- liaises with the Trustees.
- meets regularly with the Online Safety Lead and responsible Trustee to discuss current issues, review incident logs and filtering and change control logs.
- reports regularly to Senior Leadership Team.

Digital Lead and IT Technical Staff

Where the school procures IT services from an outside contractor, it is the responsibility of the school to ensure that the service provider observes all the online safety measures expected of the school technical staff, as suggested below. The school will make outside contractors aware if online safety policy and procedures in advance of them carrying out work.

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any National Cyber Security Centre and RPA online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced device management and password protection policy.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template")
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks, laptop, internet and digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Heads of Year and Online Safety Lead for investigation/action/sanction or escalated according to the school's behaviour policy.
- that monitoring software/systems are implemented and updated as agreed in school policies.

All Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the Online Safety Lead, Digital Lead or Pastoral Lead for investigation/action/sanction as appropriate.
- all digital communications with students, parents and carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the Online Safety Policy and acceptable use agreements.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, laptops, mobile devices, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Trustees.

Members of the Online Safety Group will assist the Online Safety and Digital Leads with:

- the production, review and monitoring of the school online safety policy and documents.
- mapping and reviewing the online safety and digital literacy curricular provision – ensuring relevance, breadth and progression.
- consulting stakeholders – including students, staff and parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Students:

- are responsible for using the school digital technology systems in accordance with the student acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations[1]
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices including use as cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet, IT and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through information evenings, parent bulletins, online safety resources, website, social media and information about national/local online safety campaigns literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and cyber hygiene and to follow guidelines on the appropriate use of:

- their children's personal loan devices inside and outside of the school
- access to parents' sections of the website and on-line student records

Community Users/Guest Access

Community and guest users who access school systems or networks as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning our online safety curriculum, we have referred to[iv]:

- DfE Teaching Online Safety in Schools
- Education for a Connected World Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum as part of Computing/Life Studies/Media Literacy & other lessons and will be regularly revisited (see appendix for details)
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutor-time activities across all years
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.

[1] https://kids.kiddle.co/Copyright?scrlybrkr=6c5e3966

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents and carers

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Newsletters, web site, National Online Safety courses
- National Cyber Security Centre resources
- Parent information sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (see appendix for further links/resources)

Education & Training – Staff including volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly**.
- **All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.**
- The Online Safety coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to staff in meetings/training sessions.
- The Online Safety and Digital Leads will provide advice, guidance and training to individuals as required.

Training – Trustees

Trustees should take part in online safety training and awareness sessions, with particular importance for those who are members of any group involved in technology, online safety, health and safety and safeguarding.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

A more detailed Technical Security Template Policy can be found in the appendix.

- School technical systems will be managed in ways that ensure that the school/ meets recommended technical requirements as set out in the National Cyber Security Centre's Cyber Essentials
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by IT Services who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- The administrator passwords for the school systems, used by the Network Manager (or other authorised person) must also be available to the Executive Headteacher, Head of School and Deputy and kept secure in the school safe.
- The Digital Lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details).
- Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet**.** N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- The school has provided differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users – staff and students.)
- School technical staff may monitor and record/report the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. These systems include but are not limited to Securly, Securus and Impero
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).[v]
- Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Appropriate Business Roles will be ascribed in Arbor and access to Office 365 resources restricted.
- **Users (students or staff) may not install software to school devices without prior reference to IT Services.**
- **Use of removable media (e.g. memory sticks/CDs/DVDs) is strictly prohibited on all school devices and for any school data or personal information. This applies to student and staff users on school devices.**
- **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**. (see School Personal Data Policy Template in the appendix for further detail)

Mobile Technologies Policy (inc. BYOD/BYOT)

All Perins School students have a laptop provided through the laptop scheme or are able to access a loan device as required to support their learning. At Sun Hill Junior School, students have supervised access to Chromebooks as appropriate to learning.

Mobile technology devices may also include school owned/provided or privately owned smartphones, tablets, notebooks/laptops or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

When using mobile technologies, it is key that the students, staff and wider school community understand that the primary purpose of having a device at school is educational/employment and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy sits within the online safety policy and should be considered in the context of a range of other polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies is included in the online safety education programme. Staff receive training on cyber security and digital hygiene.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases, and communities of interest. By effectively maximizing the use of such resources, the schools recognise that not only do we have the opportunity to deepen student learning, but can also develop digital literacy, fluency and citizenship in students that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks we have considered in the use of mobile technologies. These include security risks in allowing connections to our school networks, filtering of personal devices, breakages and repairs, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

- The school acceptable use agreements for staff, students and parents gives consideration to the use of mobile technologies both in school and offsite.
- The school does not permit students to use devices other than the school-owned scheme laptops while in school. This is to ensure that everyone has equal access to platforms, software, technologies and also support and repair facilities. Other policies prohibit the use of mobile phones by students in school.
- Staff are issued with a device appropriate to their role. Where staff wish to use personal devices to access school data and systems both in school and outside, these devices will be partly managed by the school's technological systems or a mobile device management profile.
- In order to protect the personal information of our students, staff and stakeholders, we have in place strict rules that prohibit the use of personal devices to capture, edit, store or process images and video. School-owned devices which are fully managed are available for these uses where appropriate.

	School Devices		Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	✓	✓	No[2]	Yes/No[2]	✓[2]
Full network access	✓	✓	-	No	No
WiFi/Internet only	✗	✗	-	✓	✓
No network access	-	-	✓	✓	✓

- The school has provided technical solutions for the safe use of mobile technology for school personal devices:
  - All school devices are controlled though the use of Mobile Device Management software or policies.
  - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
  - The school manages and regularly reviews broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
  - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted.
  - Appropriate exit processes are implemented for devices no longer used at the school or by an authorised user. Where students are offered the option to purchase their ex-scheme laptop, a prescribed process is in place to remove all school owned software and licences and any management software. The device is completely removed from the school network.
  - All school devices are subject to routine monitoring.
  - Pro-active monitoring has been implemented to monitor activity using Securus, Securly and Impero systems.
  - When staff personal devices are permitted:
  - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access.

[2] The school/academy should add below any specific requirements about the use of personal devices in the school/academy e.g. storing in a secure location, use during the day, liability, taking images etc

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in school. It is not permitted to use personal devices are to capture, edit, store or process images or video.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged personal devices while at school or on activities organised or undertaken by the school.
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable. Student laptops must be kept in the supplied protective case to help secure them as the devices are moved around the school.
- Passcodes or PINs should be set on personal devices to aid security.
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school.
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day.
- School devices are provided to support learning. It is expected that students will bring devices to school as part of their essential equipment for learning.
- Confiscation and searching - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted.
- The software originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- The school will ensure that devices contain the necessary apps for schoolwork. Operating systems and apps installed by the school will remain licensed to the school and will not be accessible to students or staff on authorised devices once they leave the school roll or employment. Any apps purchased by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity and only on a school owned device. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher direction.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.
- Printing from students and personal devices will not be possible.

Damage Cover

Devices provided to students under the Laptop Scheme have full warranty and limited damage cover. Staff devices have full warranty and may be covered by the school's insurance for theft or total loss. Each claim would be considered individually.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press (covered as part of the AUA signed by parents or carers at the start of the year - see parents/carers acceptable use agreement in the appendix)
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records. See the Perins School policies page
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)

- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible.to learners.
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any school owned mobile device the:

- data must be encrypted, and password protected.
- device must be password protected.
- device must be protected by up-to-date operating system, virus and malware checking software.
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school.
- where personal data is stored or transferred on mobile or other devices these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy.
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	✓							✓
Use of mobile phones in lessons			✓					✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones/cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails								✓
Use of messaging apps			✓					✓
Use of social media			✓					✓
Use of blogs			✓					✓

When using communication technologies, the school considers the following as good practice:

- The official school email and Teams messaging services may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email and Teams services to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to any member of school staff in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- The school uses an anonymous reporting app Whisper – https://boost.swgfl.org.uk/
- **Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students will be provided with individual school email address for educational use.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers

Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

The school includes these aspects of their policy in the staff and student acceptable use agreements.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. https://boost.swgfl.org.uk/
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff. Where students are included in social media posts, their first name and second initial only will be used. Images will only be used where the appropriate consents have been sought and given.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority/MAT.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Official school social media accounts are established and the procedures for managing these include:

- A process for approval by senior staff.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

The school's use of social media for professional purposes will be checked regularly by the senior safeguarding lead and Online Safety Group to ensure compliance with the school policies.

The school uses SWGfL Reputation Alerts that highlight any reference to the school in online media (newspaper or social media for example) https://boost.swgfl.org.uk/

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying is also banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school/ context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. The school has referred to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						X

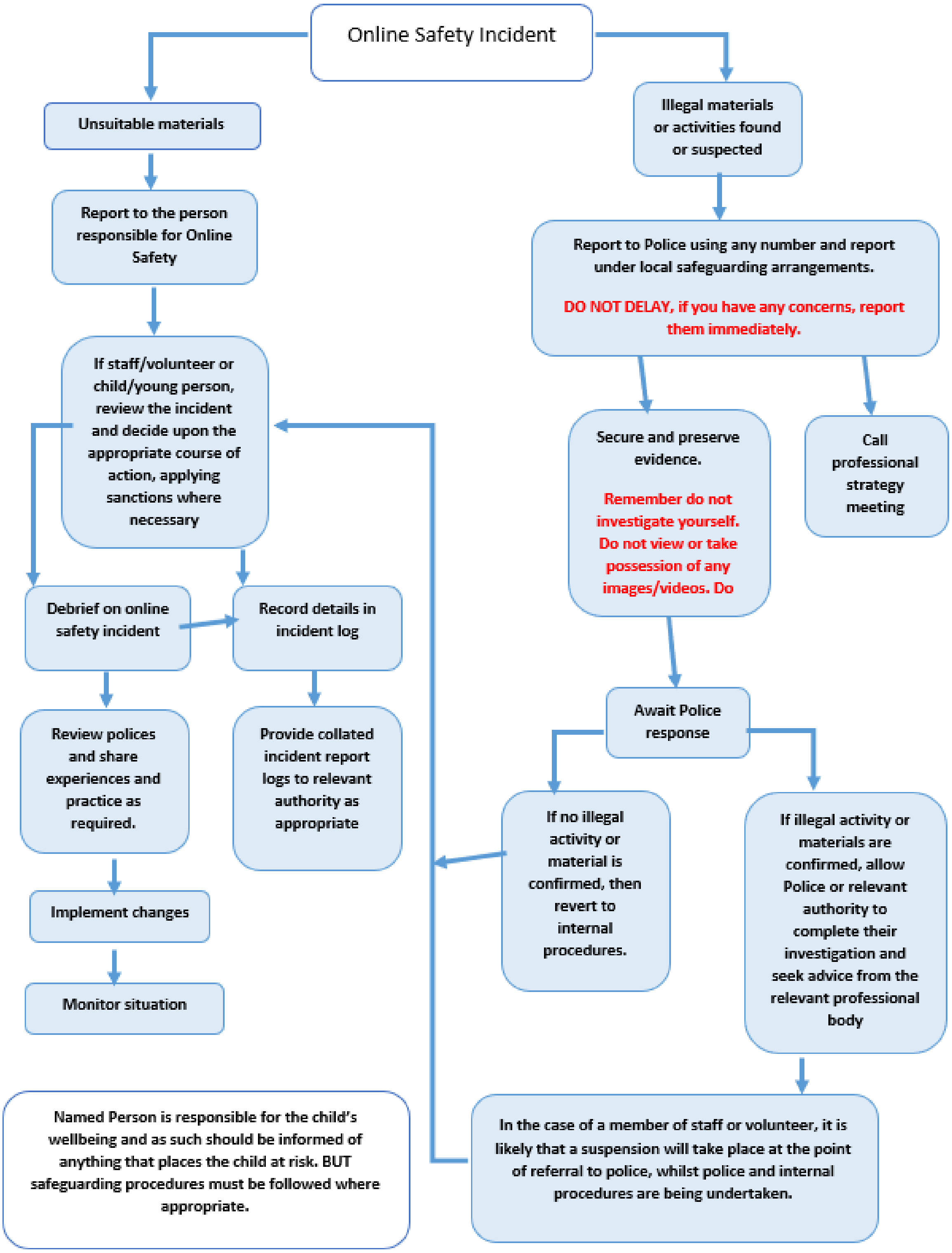
• Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	
File sharing		X			
Use of social media			X		
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures (see behaviour policy)
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police and to the MASH team would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the device in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that we will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as per our behaviour policy.

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet/social media/personal email		X	X			X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X	X		
Deliberate actions to breach data protection or network security rules	X			X	X		X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X		X	
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	X	X		X			X	
Actions which could compromise the staff member's professional standing		X	X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X		
Using proxy sites, VPNs or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				X
Breaching copyright or licensing regulations	X				X	X		
Continued infringements of the above, following previous warnings or sanctions	X				X		X	

Appendix

Appendices

Student Acceptable Use Agreement 21

Parent/Carer Acceptable Use Agreement Template 22

Staff (and Volunteer) Acceptable Use Policy Agreement 23

Responding to incidents of misuse – flow chart 26

Record of reviewing devices/internet sites (responding to incidents of misuse) 27

Reporting Log 28

Training Needs Audit Log 29

School Technical Security Policy Template (including filtering and passwords) 30

School policy template: Electronic Devices - Searching & Deletion .... **Error! Bookmark not defined.**

Social Media Policy Template 54

Online Safety Group Terms of Reference 60

Legislation 61

Links to other organisations or documents 65

Glossary of Terms 68

Audit of DfE identified areas for teaching in schools 68

Student Acceptable Use Agreement

To be included on the student homepage and agreed by all students at the start of each academic year

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems and equipment in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school

- I will only use my own personal devices (mobile phones etc.) in school if I have permission.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the form here to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. A copy of the *student/pupil* acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to complete the form below to show their support of the school in this important aspect of the school's work.

Parents are expected to countersign the Student Acceptable Use Policy

As the parent/carer of the above *students/pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

This form
The responses will be accessible to the Pastoral and Safeguarding teams
The responses will be stored electronically and encrypted in cloud storage

The responses will be deleted at the end of the academic year

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only a child's first name/initials will be used.

The school will comply with the Data Protection Act and request students (aged 12+) and/or parent's/carers permission at the beginning of each academic year for using images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names. We will seek further consent for taking and use of images for specific events that fall outside of the school's main legal basis for processing e.g. trips, performances etc.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

Parents/carers are requested to complete the consent form in Arbor to allow the school to take and use images of their children and for the parents/carers to agree.

Use of Cloud Systems

The school uses cloud systems to deliver the curriculum.

Using Microsoft 365 will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Use of Biometric Systems in England and Wales

The school collects biometric data for the operation of the cashless catering payments system. A separate and detailed data collection form is sent to parents before children join the school. The school's handling of biometric data is covered by our Data Protection Policy.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, cloud, Arbor etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. **I will not use my personal equipment to record these images**, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. I will check that every student has consent before an image is published.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner and logged against the student record in the MIS.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date operating system patches and anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have specific permission.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Handling Policy. Where digital personal data is transferred outside the secure local network, **it must be encrypted**. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

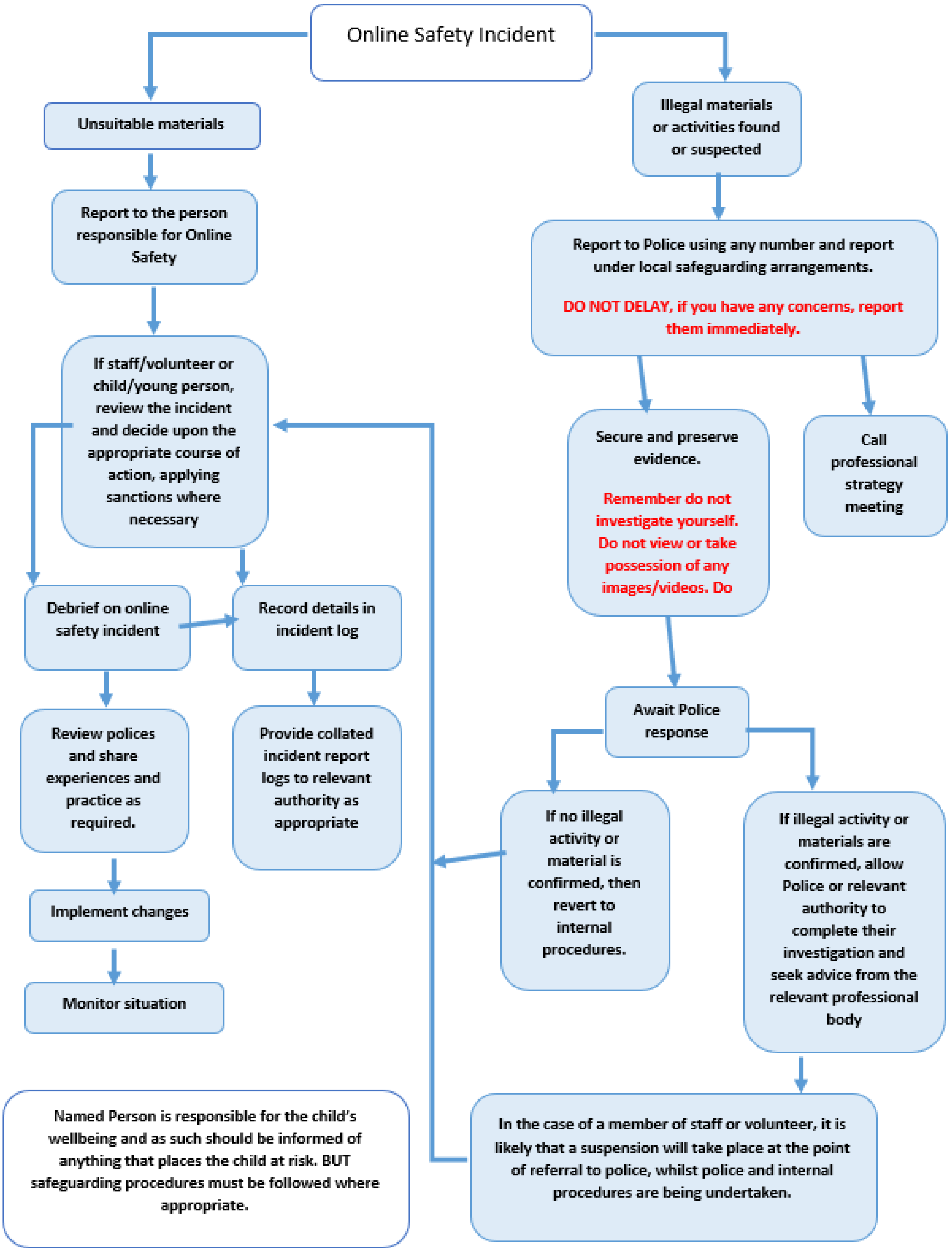
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a helpful letter, a warning, a suspension, referral to trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Responding to incidents of misuse – flow chart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: --

Date: --

Reason for investigation: --

Details of first reviewing person

Name: --

Position: --

Signature: --

Details of second reviewing person

Name: --

Position: --

Signature: --

Name and location of computer used for review (for web sites)

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: ....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log (in conjunction with CPD lead)

Group: ....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

School Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure, network and data is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system.
- there is effective guidance and training for users.
- there are regular reviews and audits of the safety and security of school computer systems.
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Core Services Manager

Technical Security

Policy statements

The school will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements set out in the National Syber Security Centre's Cyber Essentials
- there will be regular reviews and audits of the safety and security of school technical systems.
- servers, wireless systems and cabling must be securely located and physical access restricted.
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- all users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see password section below)
- The Core Services Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- mobile device security and management procedures are in place.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- remote management tools are used by staff to control workstations and view users activity
- an appropriate system is in place ITHelpdesk for users to report any actual/potential technical incident to the IT Services Team
- an agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school system. Business roles are allocated in Arbor that restrict access to minimum necessary.
- Students and staff are prohibited from downloading executable files and the installation of programmes on school devices without first having specific permission from the IT Services team.
- Staff must not allow their school devices to be used by family members or others for any purpose
- The use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices is strictly prohibited.

- the school infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

Further guidance can be found from the National Cyber Security Centre and SWGfL "Why password security is important"

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group.
- All users (adults and students/pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by IT Services who will keep an up-to-date record of users and their usernames.

Password requirements:

We follow the National Cyber Security Centre's guidance on passwords:

> User-generated passwords are quick and easy to implement and are the most common way of composing passwords. However, they carry risks that machine-generated passwords do not:
>
> - users may re-use passwords that they already use on other systems.
> - users may use easily guessed passwords (such as a pet's name)
> - users may adopt predictable password generation strategies (such as replacing the letter 'o' with a zero)
>
> This means that systems with user-generated passwords will normally contain a large number of weak passwords that will quickly fall to an automated guessing attack. Password deny listing can help to prevent the most common passwords being used.

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Passwords must not include names or any other personal information about the user that might be known by others.
- Passwords must be changed on first login to the system.
- The school recommends that staff make use of a 'password vault'. These can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.
- Passwords should not be set to expire as long as they comply with the above but should be unique to each service the user logs into.

Wherever possible we will enforce the use of multi-factor authentication. This may be more convenient for staff using personal mobile phones but there is no firm requirement to do so as alternative methods of verification will always be available.

Learner passwords:

- Records of learner usernames and passwords for **Sun Hill Junior School** pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity may be reduced but should still include upper/lower case, numbers and special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- Password requirements for students at Key Stage 2 and above should increase as they progress through school. No record of these is maintained.
- Users will be required to change their password if it is compromised.
- Students/ will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. All admin accounts will be protected using two factor authentication wherever possible.
- An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by xxxxx (insert title) (schools/colleges may wish to have someone other than the school's/college's technical staff carrying out this role e.g. an administrator who is easily accessible to users). Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. WiFi access is controlled by issuing of vouchers which expire soon after use.
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way. Please see our blog for more details on this.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement

Students will be made aware of the school's/college's password policy:

- at induction in Year 7
- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:
The responsible person (Core Services Manager) will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons to systems
- Security incidents related to this policy.

Filtering

Introduction
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Core Services Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged via change control form
- be reported to the Online Safety Lead where the reason for blocking is not clearly a false positive:
    - authorised by a second responsible person prior to changes being made.
- be reported to the Online Safety Group every term in the form of an audit of the change control logs.

All users have a responsibility to report immediately to IT Services or a Safeguarding Lead any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials. This includes the use of VPN services.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school has provided enhanced/differentiated user-level filtering through the use of Securly content filtering on student devices, *(allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)*. This is applied regardless of where the device is connected. The school also uses SurfProtect as a default filter at the point where the network is connected to the Internet with the service provider EXA.
- In the event of the technical staff needing to switch off or bypass the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or Digital Lead.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- Any filtering issues should be reported immediately to the filtering provider through IT Services.
- It is not possible to remove staff from the list of filtered users.

Education/Training/Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

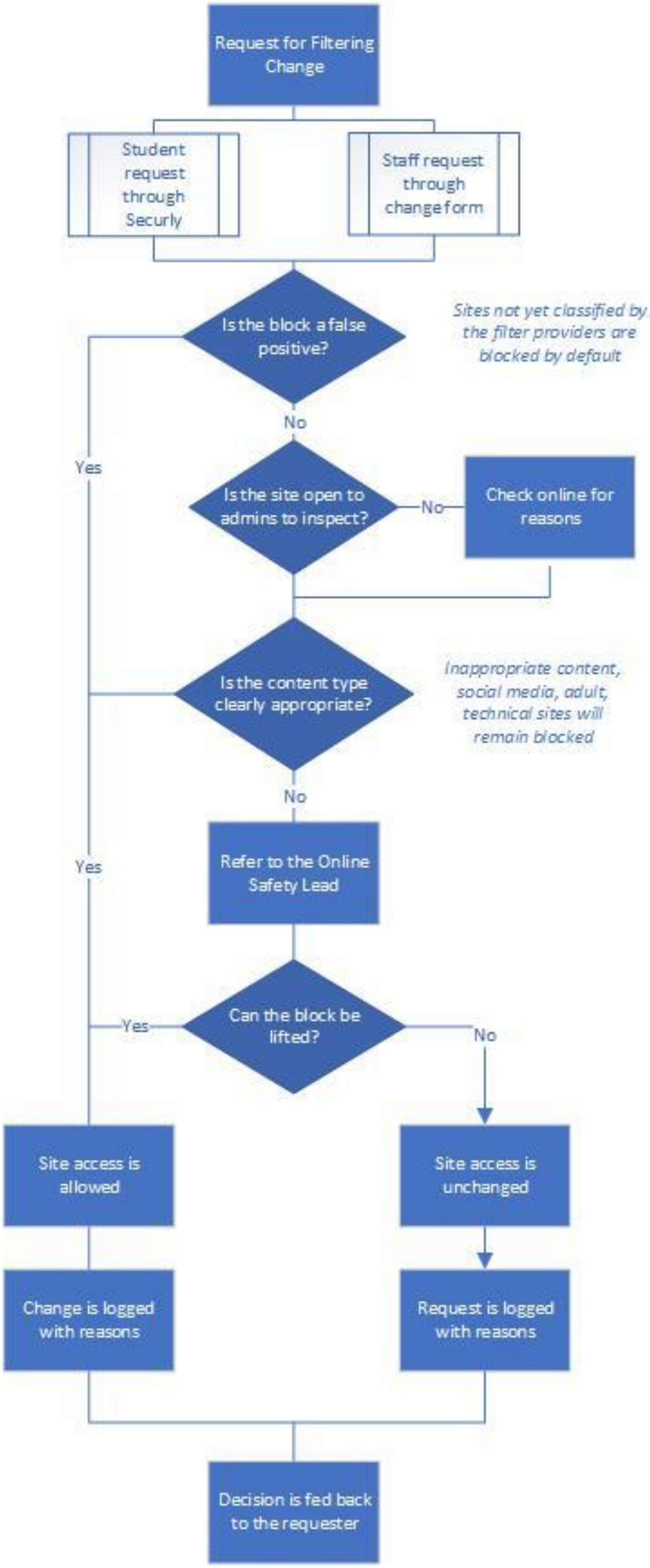
- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

Requests to allow access to blocked web content are considered individually. Users of the Securly filter can submit a request directly from the block page. The Digital Lead receives an email. The decision process is:


Request for Filtering Change
Student request through Securly
Staff request through change form
Is the block a false positive?
Sites not yet classified by the filter providers are blocked by default
No
Yes
Is the site open to admins to inspect?
No
Check online for reasons
Is the content type clearly appropriate?
Inappropriate content, social media, adult, technical sites will remain blocked
No
Yes
Refer to the Online Safety Lead
Can the block be lifted?
Yes
No
Site access is allowed
Site access is unchanged
Change is logged with reasons
Request is logged with reasons
Decision is fed back to the requester

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to IT Services or DSL who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. Monitoring is provided by a combination of Securus 360 and Securly. Securly alerts the school when a website or search term of concern is identified. These are forwarded to Heads of Year to follow up. Securus monitors content from the student laptop and captures a screenshot of any activity that meets the keywords list. These captures are reviewed by the Online Safety Lead. In addition, the school subscribes to Securus' Fully Managed Monitoring Service (FSM). A team of safeguarding experts will monitor, analyse and alert the school to high-risk incidents of concern.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Online Safety Lead, Headteacher, Digital Lead
- Online Safety Group
- Online Safety Trustee / Students Standards Committee
- Police or other relevant agencies on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

The Department for Education 'Keeping Children Safe in Education' requires schools to: *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

Data Protection Law – A Legislative Context

This section should be read in conjunction with the school's data protection, data handling and privacy policies and notices available here.

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 – this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as; how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc.

In this document the term "Data Protection Law" refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'.

A school is, for the purposes of the Data Protection Law, a "public body" and further processes the **personal data** of numerous **data subjects** on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools/academies is available on the Information Commissioner's Office (ICO) website including information about the Data Protection Law.

The ICO's powers are wide ranging in the event of non-compliance and schools/academies must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to data subjects;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the school to put in place appropriate **privacy notices** (to give a data subject information about the personal data processing activities, **legal basis of processing** and **data subject rights**) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

Data Mapping to identify personal data, data subjects and processing activities

The school and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school has a **data map** of these activities; it can then make sure that the correct privacy notices are provided, put in place **security measures** to keep the personal data secure and other steps to avoid **breach** and also put in place data processing agreements with the third parties.

The data map should identify what personal data held in digital format or on paper records in a school/ academy, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors – and personal data of names, addresses, contact details
- Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports
- Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as '**special category**' being personal data;
"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

This should be identified separately and to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

The school will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

(a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)

(b) Contract: the processing is necessary for a contract you have with the data subject

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities' use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"* however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.

Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools/academies should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function.

Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.
- if the school requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, we apply the public task lawful base.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is.
- What personal data is being processed and the lawful purpose of this processing.
- where and how the personal data was sourced.
- to whom the personal data may be disclosed.
- how long the personal data may be retained.
- data subject's rights and how to exercise them or make a complaint.

In order to comply with the fair processing requirements in data protection law, the school will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there.

Parents/carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – unlikely to be used in a school context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and academies, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

A school must not disclose personal data even if requested in a Subject Access Request;

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Your school or academy must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high-profile issue for schools, academies and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools/academies are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any-personal data breach

Schools / academies have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools / Academies will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO.

The school should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

The school should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of personal data

The school should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the personal data

Fee

The school should pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the school to a penalty in additional to other fines possible under the Data Protection Law.

Responsibilities

Every maintained school is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks

- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with Data Protection Law

The school may also wish to appoint a Data Manager. Schools/academies are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / academy's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). System Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school to consider whether the requested information should be released into the public domain. FOI links to Data Protection Law whenever a request includes personal data. Good advice would encourage the school to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/academy's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually

- ensure that a well-managed records management and information system exists in order to comply with requests
- ensure a record of refusals and reasons for refusals is kept, allowing the school to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's / academy's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools / academies complete the Guide to Information for Schools.

Parental permission for use of cloud hosted services

Schools/academies that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools/academies that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools/academies under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Law
- They must provide alternative means for accessing services where a parent or pupil has refused consent

Advice to schools/academies makes it clear that they are not able to use pupils' biometric data without parental consent. Schools/academies may wish to incorporate the parental permission procedures into revised consent processes. (see Appendix Parent / Carer Acceptable Use Agreement)

Privacy and Electronic Communications

Schools/academies should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (updated with new DfE guidance – September 2022)

The DfE guidance – Searching, Screening and Confiscation was updated in July 2022.

Please note this guidance pertains only to schools in England.

Introduction

The changing face of information technologies and ever-increasing learner use of these technologies has meant that the Education Acts were updated to keep pace. Part 2 of the Education Act 2011 (Discipline) introduced changes to the powers afforded to schools by statute to search learners in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to screen, confiscate and search for items 'banned under the school rules' and the power to 'delete data' stored on confiscated electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question relates to an offence and/or may be used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, **if they think there is a good reason to do so** (see later section)

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents/carers and learners at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for schools" (**updated July 2022**)

The DfE Guidance – "Behaviour in Schools" was updated in July 2022 and refers to behaviour online:

> "The way in which pupils relate to one another online can have a significant impact on the culture at school. Negative interactions online can damage the school's culture and can lead to school feeling like an unsafe place. Behaviour issues online can be very difficult to manage given issues of anonymity, and online incidents occur both on and off the school premises. Schools should be clear that even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity.
>
> Inappropriate online behaviour including bullying, the use of inappropriate language, the soliciting and sharing of nude or semi-nude images and videos and sexual harassment should be addressed in accordance with the same principles as offline behaviour, including following the child protection policy and speaking to the designated safeguarding lead (or deputy) when an incident raises a safeguarding concern.
>
> Many online behaviour incidents amongst young people occur outside the school day and off the school premises. Parents are responsible for this behaviour. However, often incidents that occur online will affect the school culture. Schools should have the confidence to sanction pupils when their behaviour online poses a threat or causes harm to another pupil, and/or could have repercussions for the orderly running of the school, when the pupil is identifiable as a member of the school or if the behaviour could adversely affect the reputation of the school.
>
> Headteachers should decide if **mobile phones** can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks.
>
> If headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school's behaviour policy, should outline the approach to mobile phones and be reiterated to all pupils, staff and parents throughout the school year. Headteachers should ensure it is consistently and fairly applied."

A new Keeping Children Safe in Education guidance document is in force from September 2022. Schools should be aware of new guidance concerning **Harmful Sexual Behaviour** (see policy template in these appendices):

> "Following any report of child-on-child sexual violence or sexual harassment offline or online, schools should follow the general safeguarding principles set out in Keeping children safe in education (KCSIE) - especially Part 5. The designated safeguarding lead (or deputy) is the most appropriate person to advise on the school's initial response. Each incident should be considered on a case-by-case basis.

> Schools should be clear in every aspect of their culture that sexual violence and sexual harassment are never acceptable, will not be tolerated and that pupils whose behaviour falls below expectations will be sanctioned. Schools should make clear to all staff the importance of challenging all inappropriate language and behaviour between pupils. Schools should refer to the Respectful School Communities toolkit for advice on creating a culture in which sexual harassment of all kinds is treated as unacceptable."

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: insert relevant names/roles/group

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: (the policy should here list those staff/roles given such authority. A Headteacher may choose to authorise all staff willing to be authorised, but should consider training needs in making this decision).

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training/Awareness

Members of staff will be made aware of the school's policy on "Electronic devices – searching, confiscation and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Screening

DfE "Screening, searching and confiscation – Advice for schools" allows schools to use screening: Please refer to the school's behaviour policy for details.

The school **Behaviour Policy** refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

Learners are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.

If learners breach these rules the sanctions can be found in the Behaviour Policy

School Online Safety Policy – Harmful Sexual Behaviour

Background context and legislation.

Introduction

Legislative background and context

Key Documents:

- Department for Education: Keeping Children Safe in Education
- Department for Education: Sexual violence and sexual harassment between children in schools and colleges
- Everyone's Invited
- Department for Education: Sharing Nudes and Semi-Nudes: Advice for Education Settings working with Young People
- Ofsted: Review of sexual abuse in schools and colleges
- Department for Education: Teaching Online Safety in Schools
- Department for Education: Working together to safeguard children
- Report Harmful Content: Laws about harmful behaviours

In March 2021 it was discovered that the Everyone's Invited website was holding "testimonials" about incidents that occurred in over 3000 schools in the UK. This highlighted a wide range of abuse scenarios involving children abusing other children. As a result, the Education Secretary requested a rapid review into sexual abuse in schools and colleges in England. Ofsted published their findings in June 2021. This led to a series of recommendations for schools, multi-agency partners and government.

Ofsted's School Inspection Handbook states that:

> "leaders ensure that their school's culture addresses harmful sexual behaviour. **Inspectors will expect schools to assume that sexual harassment, online sexual abuse and sexual violence are happening in the community, and potentially in the school, even when there are no specific reports, and put in place a whole-school approach to address them."**

> "Schools should have appropriate and well-communicated school-wide policies in place that make it clear that sexual harassment, online sexual abuse and sexual violence (including sexualised language) are unacceptable."

Ofsted will:

- Request that college leaders supply records and analysis of sexual harassment and sexual violence, including online, to inspectors. The Independent Schools Inspectorate will also specifically request schools to provide the same records upon notification of inspection, in addition to its current practice.
- Speak with groups of pupils, where this helps them to better understand a school or college's approach to tackling sexual harassment and violence, including online.
- Feed this part of the inspection into a judgement of safeguarding and leadership and management. If a school's processes are not adequate, Ofsted is likely to judge both their safeguarding practices and leadership and management as inadequate.

Your behaviour and safeguarding/child protection policies will likely be checked to see whether they set out clear and effective procedures to prevent and respond to incidents. It will be expected that you have a zero-tolerance approach to all harmful sexual behaviour.

Online:

Policy for Harmful Sexual Behaviour

Statement of intent

Our school has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledge that it could be occurring at *(insert name of school)* and in our school community. The school is proactive in its approach to assessing prevalence, responding to incidents and challenging and changing behaviour. This policy applies to all volunteers, trustees, staff and learners.

Schools and colleges have a statutory duty to safeguarding the children in their setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our whole-school approach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat everything as safeguarding incident in the first instance - we distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As a school we provide regular opportunities for school staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.

Related policies

This policy should be read in conjunction with:

- Child protection and safeguarding policy
- Whistleblowing
- Behaviour policy
- Anti-bullying policy
- Online safety
- Acceptable Use Agreements
- Curriculum Policies
- Use of outside agencies
- Add any other polices that may be relevant

Definitions

As stated in the Sexual Offences Act 2003, the term Harmful Sexual Behaviour (HSB) covers a wide range of behaviours, often these may be considered problematic, abusive, or violent and may also be developmentally inappropriate. HSB can occur online, offline or in a blend of both environments. The term HSB is widely acknowledged in child protection and should be treated in this context.

Whilst peer on peer harassment has become a widely recognised term, this is already moving towards child on child in recognition that age and development is a factor in making decisions about behaviour. A significant age difference between the children involved in an incident may lead to a decision about the behaviour being harmful or not. For example, this could be an older child’s behaviour towards a pre-pubescent child, or a younger child’s behaviour towards an older child with learning difficulties. It is important that Designated Safeguarding Leads (DSL) know what is and is not HSB. DSLs should be involved in planning the curriculum for HSB, planning preventative actions and ensuring a whole-schools culture that condones HSB, alongside all other forms of abuse and harassment. This template policy provides a basis for an effective approach to managing sexual violence and harassment.

What is sexual violence?

The following are sexual offences under the Sexual Offences Act 2003:

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents. (NOTE- Schools and colleges should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent, or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.)

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not reasonably believe that B consents. (NOTE – this could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

What is sexual harassment?

Keeping Children Safe in Education Guidance 2022 and the Sexual Violence and sexual harassment between children in schools and colleges state:

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school/college. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names
- sexual "jokes" or taunting
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence – it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and
- Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
- consensual and non-consensual sharing of nude and semi-nude images and/or videos. Taking and sharing nude photographs of U18s is a criminal offence.
    - sharing of unwanted explicit content
    - upskirting (this is a criminal offence)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation; coercion and threats.

It is important that schools and colleges consider sexual harassment in broad terms. Sexual harassment (as set out above) creates a culture that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

Responsibilities

Leaders and DSLs

Our leaders and DSLs have ultimate responsibility in dealing with all incidents of harmful sexual behaviour, including online. It is the expectation that all incidents of harmful sexual behaviour/sexual violence and harassment are reported in line with school safeguarding and child protection procedures.

We ensure that our designated safeguarding lead/s (DSL) and their deputies are confident in school safeguarding processes and when it is necessary to escalate. Our DSLs know what local and national specialist support is available to support all children involved in harmful sexual behaviour and are confident as to how to access this support when required.

Designated safeguarding lead/s and their deputies have an in-depth working knowledge of key documentation, particularly KCSIE 2022 and Sexual Violence and Sexual Harassment Between Children in Schools and Colleges (DfE 2021). We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

It is the role of school leaders and designated safeguarding leads to ensure that all staff and Governors receive training specific to harmful sexual behaviour, and that it is included as part of induction.

Staff

It is the responsibility of all staff to have read and understood this policy and associated policies. All staff must report any incidents or suspected incidents of harmful sexual behaviour to DSLs in line with school policy and ensure they are informed of the outcome. All staff will challenge any harmful sexual language or inappropriate behaviour. Staff have a duty to ensure that the school environment is one which is safe and which supports learners to understand safe and healthy relationships and appropriate behaviour through delivery of our curriculum.

Governors

We ensure that our trust board/governing body have a good understanding of what harmful sexual behaviour is, when it can pose a risk to children and how to keep children safe. Our trustees/governors receive regular training and updates, both in terms of what sexualised behaviour is, but also how to effectively support establishments and their stakeholders whilst holding provision to account.

As part of the headteacher's report, our trust board/governing body has the opportunity to monitor and evaluate the approach to harmful sexual behaviour to ensure it is adequate and effective. This includes evaluation of the curriculum, pupil voice activity and evaluation of parent/carer engagement. Trustees/Governors ensure that risks relating to these issues are identified, that a number of reporting routes are available, and that risks are effectively mitigated.

Learners

All learners have the right to learn in a safe, healthy and respectful school environment. Our learners benefit from a broad and balanced curriculum and are taught about healthy relationships and know how and when to report and that a range of different reporting routes is available to them. Our learners are encouraged to report any harmful sexual behaviour, even if they are not directly involved. All learners will be believed if they make a disclosure and will be treated sensitively - whilst we cannot guarantee confidentiality, their thoughts and wishes will be taken into account when supporting them.

Parents/carers

We work hard to engage parents and carers by:

- regular in school sessions
- sharing newsletters
- sharing information online e.g., website, social media
- providing curriculum information
- List any other ways you may engage parents and carers e.g.

Our parents and carers are made aware of how and when to report any concerns to the school, that all incidents will be handled with care and sensitivity, and that it may sometimes be necessary to involve other agencies.

Vulnerable groups

We recognise that, nationally, vulnerable learners are three times more likely to be at risk from Harmful Sexual Behaviour. These include:

- A child with additional needs and disabilities.

- A child living with domestic abuse.
- A child who is at risk of/suffering significant harm.
- A child who is at risk of/or has been exploited or at risk of exploited (CRE, CSE),
- A care experienced child.
- A child who goes missing or is missing education.
- Children who identify as, or are perceived as, LGBTQI+ and/or any of the other protected characteristics

Children displaying HSB have often experienced their own abuse and trauma. We ensure that any vulnerable learner is offered appropriate support, both within and outside school, sometimes via specialist agencies.

Reporting

Our systems are well promoted, easily understood and easily accessible for children and young people to confidently report abuse, knowing their concerns will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- online reporting tool,
- links to national or local organisations
- list any other systems here
- speaking to any member of staff

Responding to an incident or disclosure

In this policy we recognise the importance of distinguishing between healthy, problematic and sexually harmful behaviour (HSB)

Our response is always based on sound safeguarding principles and follows school safeguarding processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

The school will always adopt a multi-agency approach and seek external support and guidance, in line with school policy, if deemed necessary. This may include:

List relevant agencies e.g., MASH, Early Help, CAMHS, Police etc

Risk assessment

The school may deem it necessary to complete a harmful sexual behaviour risk assessment as part of the response to any reported incidents. The purpose of the risk assessment is the protect and support **all those involved** by identifying potential risk, both in and out of school (e.g., including public transport, after school clubs etc) and by clearly describing the strategies put in place to mitigate such risk.

The risk assessment will be completed following a meeting with all professionals working with the learner, as well as parents or carers. Where appropriate, the learners involved will also be asked to contribute.

The risk assessment will be shared will all staff who work with the learner, as well as parents and carers. It will be dynamic and will respond to any changes in behaviour and will be regularly evaluated to assess impact.

Education

Our school's educational approach seeks to develop knowledge and understanding of healthy, problematic and sexually harmful behaviours, and empowers young people to make healthy, informed decisions. Our school's approach is delivered predominantly through PSHE and RSE and additional opportunities are provided through:

- Cross curricular programmes (e.g., using the ProjectEVOLVE resources)
- Computing
- Transform, Life Studies, Assemblies

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our setting. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this by any of:

- Surveys
- Focus groups
- Parental engagement
- Staff consultation
- Staff training

The following resources are used:

- ProjectEVOLVE - https://projectevolve.co.uk
- List other resources which are used to deliver the curriculum here

Training

It is effective safeguarding practice for the designated safeguarding lead (and their deputies) to have a good understanding of HSB. This could form part of their safeguarding training. This will aid in planning preventative education, implementing preventative measures, drafting and implementing an effective child protection policy and incorporating the approach to sexual violence and sexual harassment into the whole school or college approach to safeguarding.

- Brook traffic light tool
- NSPCC training
- Whole staff training
- List other training the school has undertaken

A clear training strategy which supports staff to respond effectively to different types of harassment and sexual misconduct incidents. This should involve an assessment of the training needs of all staff. This strategy should be reviewed and evaluated on a regular basis to ensure it is fit for purpose.

Training should be made available on an ongoing basis for all staff and students to raise awareness of harassment and sexual misconduct with the purpose of preventing incidents and encouraging reporting where they do occur.

Links

Child Exploitation and Online Protection command: CEOP is a law enforcement agency which aims to keep children and young people safe from sexual exploitation and abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors

The NSPCC provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support for school and college staff and will be especially useful for the designated safeguarding lead (and their deputies)

Support from specialist sexual violence sector organisations such as Rape Crisis or The Survivors Trust

The Anti-Bullying Alliance has developed guidance for schools about Sexual and sexist bullying.

The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues

Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)

Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

UKCIS Sharing nudes and semi-nudes advice: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).

Thinkuknow from NCA-CEOP provides support for the children’s workforce, parents and carers on staying safe online

Lucy Faithful Foundation

Marie Collins Foundation

NSPCC National Clinical and Assessment Service (NCATS)

Project deSHAME from Childnet provides useful research, advice and resources regarding online sexual harassment.

Social Media Policy Template

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Perins School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation
- **Administrator/Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school has official social media accounts, managed by the marketing team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

The creation of social media accounts or any other online presence in the name of, or connected to the school is subject to:

Anyone wishing to create an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

All applications will be considered in the context of the wider school, it's aims and objectives.

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account. Any request for information that may constitute a subject access request must be logged and passed to the Data Protection Officeer as there is a firm deadline for response.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must pass this onto the Senior Leadership Team and not respond themselves unless directed to do so.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
  - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
  - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
  - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- **Students**
  - **Staff are not permitted to follow or engage with current students of the school on any personal social media network account.**
  - The school's education programme should enable students to be safe and responsible users of social media.
  - Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's/academy's behaviour policy.
- **Parents/Carers**
  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's/academy's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Don’t use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do’s

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school’s reporting process
- Consider turning off tagging people in images where possible

The Don’ts

- Don’t make comments, post content or link to materials that will bring the school into disrepute
- Don’t publish confidential or commercially sensitive material
- Don’t breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
- Don’t post derogatory, defamatory, offensive, harassing or discriminatory content
- Don’t use social media to air internal grievances

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

Socials cheat sheet for staff

Do not accept friend requests from students on social media

10 rules for school staff on social media platforms

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling social media apps from your phone. Many of these recognise WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as students)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** –find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Search your name** online to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** –find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify the school safeguarding team. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:

    - Responding to one parent’s friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Students may then have indirect access through their parent’s account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you’re doing so

You’re being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- **Report the incident to the school’s safeguarding team**
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the social media provider or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the [school] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include

- SLT member/s
- Child Protection/Safeguarding lead
- Teaching staff member
- Support staff member
- Online safety coordinator
- Trustee
- Parents/Carers
- ICT Technical Support staff
- Student representation – for advice and feedback. Student voice is essential in the make-up of the online safety group, but students would only be expected to take part in committee meetings where deemed relevant.

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. Duration of Meetings

Meetings shall be held one each term. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through
    - Staff meetings
- Student forums (for advice and feedback)
- Trustee meetings
- Surveys/questionnaires for students parents/carers and staff

- Parent Information evenings
- Website/ Digital Wellbeing Newsletters
- Online safety events
- Safer Internet Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for The Perins MAT have been agreed:

Signed by: --

Date: --

Date for review: --

Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Legal advice will be sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

School/academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUA	Acceptable Use Agreement
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

Audit of DfE identified areas for teaching in schools

taken from Teaching online safety in schools (non-statutory guidance)

Description	Curriculum area(s)	Yr
• that age verification exists and why some sites require a user to verify their age. For example, online gambling and purchasing of certain age restricted materials such as alcohol, • why age restrictions exist - for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers, • helping pupils understand how this content can be damaging to under-age consumers, • the age of digital consent -the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations. Why it is important and what it means in practice.	Cz talks about age-related rights, but not with whole cohort Data protection comes up briefly in Media Literacy, summer term	9 8
• what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications, • how cookies work, • how content can be shared, tagged and traced, • how difficult it is to remove something a user wishes they had not shared, • ensuring pupils understand what is illegal online, especially what may in some cases be seen as "normal" behaviours, for example youth-produced sexual imagery (sexting). This could include copyright, sharing illegal content such as extreme pornography or terrorist content as well as the illegality of possession, creating or sharing any explicit images of a child even if created by a child.	Digital Footprint covered in Year 7 Computing, Term 1. Content shared, tagged and traced is covered in Year 7 Computing, Term 1. The last bullet point is covered in Life Studies at different points. Media Lit (Y8) includes a lesson about data, but doesn't cover all of this. Y8 Life mentions first bullet point during Careers topic, but briefly.	7 7 Images – 8, 10, 11 Porn – 11 Terror – 9, 10
• disinformation and why individuals or groups choose to share false information in order to deliberately deceive, • misinformation and being aware that false and misleading information can be shared inadvertently, • online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons,	All covered in Media Literacy – consequences less so than others Cyber Security unit in Year 8 Computing includes phishing, misinformation and fraud/scams.	8

• explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online, • how to measure and check authenticity online, · the potential consequences of sharing information that may not be true.		
• how to look out for fake URLs and websites, • ensuring pupils understand what secure markings on websites are and how to assess the sources of emails, • explaining the risks of entering information to a website which isn't secure, • what to do if harmed/targeted/groomed as a result of interacting with a fake website or scam email. Who to go to and the range of support that is available	First one briefly in Y7 Life Cyber Security unit in Year 8 Computing includes phishing, misinformation and fraud/scams.	
• what identity fraud, scams and phishing are, • that children are sometimes targeted to access adults data, for example, passing on their parents or carers details (bank details, date of birth, national insurance number etc). Therefore there is a need to keep everyone's information secure not just their own, · what "good" companies will and won't do when it comes to personal details, for example a bank will never ask you to share a password or move money into a new account.	Cyber Security unit in Year 8 Computing includes phishing, misinformation and fraud/scams.	
• why passwords are important, how to keep them safe and that others may try to trick you to reveal them, • explaining how to recognise phishing scams, for example those that seek to gather login in credentials and passwords, • importance of online security to protect against viruses (such as keylogging) that are designed to access/steal/copy passwords information, · what to do when a password is compromised or thought to be compromised.	These points are covered in Year 7 Computing term 1 (but not then revisited)	
• how cookies work, • how data is farmed from sources which look neutral, for example websites that look like games or surveys that can gather lots of data about individuals,	Data covered in one Y8 Media Lit lesson	

• how, and why, personal data is shared by online companies. For example data being resold for targeted marketing by email/text (spam), • how pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential, • the rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR), • how to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time		
• explaining that the majority of games and platforms are businesses designed to make money. Their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue, • how designers use notification to pull users back online	Video Game advertising unit in GCSE Media Studies	Yr9
• how to find information about privacy setting on various sites, apps, devices and platforms, • explaining that privacy settings have limitations, for example they will not prevent someone posting something inappropriate.	Briefly covered in Year 7 Computing.	
• how adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts, • how the targeting is done, for example software which monitors online behaviour (sites they have visited in the past, people who they are friends with etc) to target adverts thought to be relevant to the individual user, • the concept of clickbait and how companies can use it to draw people onto their sites and services	Algorithms mentioned	
• explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation, • explanation of when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail,	First two bullet points covered in Life Studies; hate crime in Y9, abuse covered at various points in each year	

• how to respond to online abuse including how to access help and support, • how to respond when the abuse is anonymous, • discussing the potential implications of online abuse, including implications for victims, • being clear what good online behaviours do and don't look like.		
• explaining what an online challenge is and that while some will be fun and harmless, others may be dangerous and or even illegal, • how to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why, • explaining to pupils that it is ok to say no and not take part, • how and where to go for help if worried about a challenge, • understanding the importance of telling an adult about challenges which include threat or secrecy ('chain letter' style challenges).		
• ensuring pupils know that online content (sometimes gang related) can glamorise the possession of weapons and drugs, • explaining that to intentionally encourage or assist an offence is also a criminal offence, • ensuring pupils know how and where to get help if worried about involvement in violence.	First point touched upon in Y7 Life	
• explaining that in some cases profiles may be people posing as someone they aren't (i.e. an adult posing as a child) or may be "bots" (which are automated software programs designed to create and control fake social media accounts), • how to look out for fake profiles. This could include - profile pictures that don't like right, for example of a celebrity or object, - accounts with no followers or thousands of followers; and - a public figure who doesn't have a verified account.	Both points mentioned in Media Lit (Y8)	
• boundaries in friendships with peers and also in families and with others,	Grooming mentioned in Y8 and 9 Life	

• key indicators of grooming behaviour, • explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult; and • how and where to report it both in school, for safeguarding and personal support, and to the police. Where there are concerns about sexual abuse and exploitation these can also be reported to Click CEOP. See the NCA-CEOP Thinkuknow website for further information on keeping children safe from sexual abuse and exploitation. At all stages it will be important to balance teaching children about making sensible decisions to stay safe whilst being clear it is never the fault of a child who is abused and why victim blaming is always wrong.		
• explaining the risks of carrying outlive streaming. These include the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent. As such pupils should think carefully about who the audience might be and if they would be comfortable with whatever they are streaming being shared widely, • online behaviours should mirror offline behaviours and considering any live stream in that context. Pupils shouldn't feel pressured to do something online that they wouldn't do offline. Consider why in some cases people will do and say things online that they would never consider appropriate offline, • explaining the risk of watching videos that are being live streamed, for example there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance.		
• that pornography is not an accurate portrayal of adult sexual relationships, • viewing pornography can lead to skewed beliefs about sex and in some circumstances can normalise violent sexual behaviour, • that not all people featured in pornographic material are doing so willingly, i.e revenge porn or people trafficked into sex work.	All in Y11 Life	
• explaining that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with, • identifying indicators or risk and unsafe communications, • identifying risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before,		

• explaining about consent online and supporting pupils to develop strategies to confidently say “no” to both friends and strangers online.		
• exploring the use of image filters and digital enhancement, • exploring the role of social media influencers, including that they are paid to influence the behaviour (particularly shopping habits) of their followers, • looking at photo manipulation including discussions about why people do it and how to look out for it.	First and third points in Y7 Life, and mentioned again later on Photography study including magazine publishing in GCSE Media Image filters and digital enhancement and manipulation covered in Year 7 Computing Photoshop unit	Yr9 and Yr10
• helping pupils to evaluate critically what they are doing online, why they are doing it, and for how long (screen time). This could include reference to technologies that help them to manage their time online, monitoring usage of different apps etc, • helping pupils to consider quality vs quantity of online activity, • explaining that pupils need to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or the fear of missing out, • helping pupils to understand that time spent online gives users less time to do other activities. This can lead to some users becoming physically inactive, • exploring the impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues, • explaining that isolation and loneliness can affect pupils and that it is very important for pupils to discuss their feeling with an adult and seek support, • where to get help.	First point in Y8 Media Lit; fifth and sixth to less of a degree in Y10 Life	
• how and why people can often portray an exaggerated picture of their lives (especially online) and how that can that can lead to perfect/curated lives pressures, • discussing how and why people are unkind or hurtful online, when they would not necessarily be unkind to someone face to face.	First one in Y10 Life	

• looking at strategies for positive use, • how to build a professional online profile		
Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using emotive language, videos or images. Guidance on teaching about mental health and emotional wellbeing provides useful support for teachers in handling this material.	Y10 Life Studies	

[i] Action – training and documented plan for

[ii] Action – training and documented plan for staff support and safety

[iii] Create an Online Safety Group:

[iv] Curriculum review and audit November 2022

[v] WHISPER online