Perins e-safety Policy

1. Introduction and School Context

a) This policy applies to all employees and volunteers, adult work experience, apprentices and teacher trainees within Perins School and in respect of all IT resources and equipment within the school and resources that have been made available to staff for working at home. IT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as Moodle & SIMS), school telephones and text systems, cameras and recording equipment, School website, and any other electronic or communication equipment used in the course of the employee or volunteer's work.

b) Safeguarding is a serious matter; at Perins School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner. The primary purpose of this policy is twofold:

   i. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met

   ii. To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

c) This policy is available for anybody to read on the Perins School website; upon review all members of staff will sign to agree they have read and understood both the e-safety policy and the Staff Acceptable Use Policy. Annually staff will re-agree the AUP and sign via IMPERO. Students will also sign diary to agree the Students Acceptable Use Policy. The Students Acceptable Use Policy is also in the school diary, and discussed in tutor time. Upon acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles and responsibilities

a) Governing Body.

The Governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

   i. Review this policy at least every three years and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

ii. Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use
    - Receive regular updates from the e-safety officer in regards to training, identified risks and any incidents

b) Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer as indicated below. The e-safety officer will ensure that:

i. E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents
ii. The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties
iii. All e-safety incidents are dealt with promptly and appropriately

c) E-safety officer

The day-to-day duty of e-Safety Officer is devolved to an Assistant Head *(Note: this is often a shared communication role with Assistant Head Pastoral – DSL designated Safeguarding Lead)* The e-Safety Officer will:

i. Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use
ii. Review this policy regularly and bring any matters to the attention of the Headteacher
iii. Advise the Headteacher, governing body on all e-safety matters
iv. Engage with parents and the School Community on e-safety matters at school and/or at home
v. Engage with the local authority, IT technical support and other agencies as required
vi. Retain responsibility for communication for the addition of incidents to SIMS and onto the overall Safeguarding recording document (See Perins School Safeguarding Policy) ensure staff know who to report to, to ensure the appropriate audit trail.
vii. Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical Support
viii. Make him/herself aware of any reporting function with technical e-safety measures, i.e. Impero violation log viewer by student and date/time. Also email lists of in school violations. Liaise with the Headteacher to decide on what reports may be appropriate for viewing
ix. Ensure that all staff are communicated to and are aware of e-safety issues and ensure that the AUP policy is read and understood by all staff

x. Ensure that e-safety is embedded into our curriculum: and that students are given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school

d) IT Technical Support Staff

Technical support staff are responsible for ensuring that: The IT technical infrastructure is secure; this will include at a minimum:

i. Anti-virus is fit-for-purpose, up to date and applied to all capable devices.

ii. Windows (or other operating system) updates are regularly monitored and devices updated as appropriate

iii. The reporting flowcharts for any member of staff worried about a child are contained in the Perins Safeguarding policy.

e) All Staff

All staff are to ensure that

i. All details within this policy are understood. If anything is not understood it should be brought to the attention of the e-safety officer or Designated Safeguarding Leader. The boundaries of use of IT equipment in the school are given in the Staff Acceptable Use Policy; any deviation or misuse of IT equipment or services will be dealt with in accordance with the School's Staff Disciplinary Policy.

ii. Any e-safety incident is reported to the e-Safety Officer (and an entry made on safeguarding incident log), or in his/her absence to the Headteacher to make a decision.

iii. The reporting flowcharts for any member of staff worried about a child are contained in the Perins Safeguarding policy

f) All Students

i. The boundaries of use of IT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of IT equipment or services will be dealt with in accordance with the behaviour policy

ii. E-safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

g) Parents and Carers

i. Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's information evenings, school newsletters, school website, the school will keep parents up-to-date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered. E.g. Parent meetings before contentious issues in PDL

ii. Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy in the student diary

2. Technology and its safe use

a) Network and Internet

i. Internet Filtering & Monitoring – We filter to ensure:

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites whilst in school. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.
- We monitor for assurance using Impero:
  - (as much as possible) that no inappropriate or illegal activity has taken place.
  - To add to any evidential trail for disciplinary action if necessary.

ii. Impero

We use Impero software that restricts unauthorised access to illegal websites. It also restricts access to inappropriate websites during school time; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. Sensitive violation criteria have been imposed to log any inappropriate key word searched or websites. The ITEL group, Assistant Head Pastoral and IT Support are responsible for ensuring that the filtering is appropriate and that any serious issues are brought the attention of the Headteacher.

iii. Anti Virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

b) Email

i. All Perins School staff will be provided with a school email address to enable them to perform their role effectively; this can be used to communicate with parents and pupils for any school related commitments. Staff are able to access

email outside of school hours from mobile or fixed devices and this email facility can be used to undertake school business outside of normal office hours.

ii. Students are provided with a Perins email address prefixed by Yxx according the year they started Perins e.g. y14Perinh. Students are given lessons about sensible and safe email use. We use Hampshire County Council software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

c) Security and Confidentiality

i. **Staff** must lock classrooms or offices when leaving any equipment unattended for any period of time to avoid damage or loss. Laptops should be locked away securely if left unattended.
ii. Any concerns about the security of the IT system should be raised with the IT services team
iii. Passwords: Students and staff are given training on security of their passwords. Every effort should be made by Staff to change passwords on a termly basis or if there has been a compromise, whichever is sooner. IT Support will be responsible for ensuring that passwords are changed.
iv. Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate processes by communicating with the Marketing Executive, before uploading material to the website
v. Where provided, staff must ensure that the school laptop is not accessible by others when in use at home and that it is not used inappropriately by themselves or others.
vi. Staff must ensure that their use of the schools IT facilities is in accordance with the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, usually through password protection. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with. Care should be taken when sending information, that sensitive data is not included unless necessary.

d) Social Networking

Greater detail can be found in the Perins School Social Media policy
Perins School recognises the value of social media when used in a responsible and professional way. To minimise the risks posed by online environments, to avoid loss and of productivity and to ensure that our IT resources and communications

are used only for appropriate purposes, we expect staff and students to adhere to this policy.

e) Photos and Videos

i. If Perins School provides digital cameras and other recording equipment for educational and school business use and if it is used off of the school site, it must be kept secure and safe. In the event of damage or loss, liability falls with the member of staff or department

ii. SIMS or the photo consent spreadsheet must be consulted before any image or video of any child is used publically, particularly in news letters or social media.

f) **Mobile Phones**

i. Personal mobile phones are not restricted but should not be used for personal use during lesson time, unless part of your employment, urgent or emergency situations arise. Staff should not share or use your personal mobile phone number when making contact with parents. Where used in these emergency situations and a cost is incurred, the school will provide reimbursement of the cost of any calls made.

ii. No mobile telephones, even those with hands free facilities should be used whilst driving on school business.

g) **Cyberbullying**

I. Staff in schools may become targets of cyber abuse/bullying and, like other forms of bullying, it can have a significant impact on their health, well-being and self-confidence. Protecting staff from abuse is best done within a prevention framework, including whole school policies and appropriate practices.

II. Cyber abuse/bullying may consist of threats, harassment, embarrassment, humiliation, defamation or impersonation. It may take the form of general insults, or prejudice based abuse, e.g. homophobic, sexist, racist or other forms of discrimination. It may involve email, virtual learning environments, chat rooms, websites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

III. Students are given assemblies, tutor activities and PDL lessons about cyberbullying. The main message is to take a screenshot and report it. Students are taught about the roles of a 'bystander' (knowing but not stopping someone) and an 'accessory' (forwarding on).

IV. Abuse using cyber technology can occur at any time and incidents can intrude into the victim's private life. The audience for such messages can be very large and can be reached rapidly. The content of electronically forwarded messages is hard to control and the worry of content resurfacing can make it difficult for the victim to move on.

V. Perins operates a zero tolerance policy towards direct or indirect harassment or assault against any member of staff, volunteers and governors. This includes the use of social media and other forms of electronic communications to facilitate the act.

VI. Cyberbullying and the law

While there is not a specific criminal offence called cyberbullying, activities can be criminal offences under a range of different laws, including:

-The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- Section 127 of the Communications Act 2003
- Public Order Act 1986
- The Defamation Acts 1952 and 1996

VII. It is the duty of every employer to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees. Incidents that are related to employment, even those taking place outside the hours or place of work may fall under the responsibility of the employer.

VIII. The student AUP reminds students about the rules on the use of equipment, software and network access provided by the school, the use of staff and pupil owned equipment and internet access routes, where they are used on school premises and within school hours, eg mobile phones, digital cameras and laptops

IX. Students are given assemblies on acceptable behaviour including behaviour outside of school e.g. use of social networking services and other sites, with regard to harming others and bringing the school into disrepute.

X. **Responding to incidents**

i. Staff should never retaliate i.e. personally engage with cyberbullying incidents.

ii. Staff and students are reminded to keep any records of abuse – texts, emails, voice mails, or instant messages. Take screen prints of messages or web pages. Record the time, date and address of the site.

iii. Inform the appropriate person e.g.tutor, Heads of House, Assistant headteacher, headteacher, at the earliest opportunity.

iv. Where the perpetrator is known to be a current pupil or co-worker, this should be dealt with through the school's own behaviour management / disciplinary procedures.

v. Monitoring and confiscation must be appropriate and proportionate - parents, employees and learners should be made aware in advance of any monitoring (for example, of email or internet use) or the circumstances under which confiscation might take place.

vi. A designated member of the leadership team should contact the police where it appears that a law has been broken – for example, where death threats, assault, or racially motivated criminal offences are involved. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police inquiries. School staff are of course able to report incidents directly to the police.

vii. If a potential criminal offence has been committed and the school is not able to identify the perpetrator, the police may issue a Regulation of Investigatory Powers Act 2000 (RIPA) request to a service provider, enabling them to disclose the data about a message or the person sending it.

XI. Getting offensive content taken down

i. Where online content is upsetting / inappropriate and the person(s) responsible for posting is known, the quickest way to get material taken

down is likely to be to ensure that the person who posted it understands why the material is unacceptable and to request that they remove it.

ii. If the person responsible has not been identified, or will not take the material down, the school will need to contact the host (i.e. the social networking site) to make a request to get the content taken down. The material posted may breach the service provider's terms and conditions of use and can then be removed.

iii. It is important to be clear about where the content is – for example by taking a screen capture of the material that includes the URL or web address. If you are requesting they take down material that is not illegal, be clear how it contravenes the site's terms and conditions.

iv. In cases of actual/suspected illegal content, the school should contact the police.

XII. There should be clear and detailed records of all events which must be kept up to date. Any witness statements (where appropriate) and notes of any subsequent meetings held to discuss the events should also be retained. Notes should be signed and dated.

XIII. Any evidence should be logged, and witnesses should be asked to make a record of exactly what they saw and heard at the earliest opportunity.

XIV. It is also advisable to ensure that in every case, even where a formal letter is not required, parents receive a written confirmation of the events and the headteacher's response.

XV. If the police are asked to deal with an incident as a criminal investigation, there are a number of actions that may thwart this process. Witness details should not be made known to suspected offenders or their families. Groups of witnesses or suspects should not be left together, or allowed to discuss what happened, before the police interview them. If in doubt always seek the advice of the police officer first.

h) **Sexting**

I. Sexting is a term used to describe the sharing of intimate images or video with another person.

II. Students are given age appropriate assemblies and PDL lessons regarding sexting. Students are reminded that most sexting is deliberate; the person sending the content means it to happen, however, the World Wide Web means the potential of a huge audience and of course, if a photo is uploaded and shared, it can be on there forever. Students are taught about the implications of sending images under 16 and of the potential consequences for the law and future employment (and of course the embarrassment)

III. Association of Chief Police Officers have clearly stated that young people will be treated as victims in the first instance and only extreme cases may be reviewed or looked at differently. They clearly state "First time offenders should not usually face prosecution for such activities, instead an investigation to ensure that the young person is not at any risk and the use of established education programmes should be utilised". – source www.swgfl.org.uk/sextinghelp

a) **BYOD**

i. For purposes of BYOD, "Device" means a privately owned wireless and/or portable electronic hand held equipment that includes, but is not limited to, existing and emerging mobile communication systems and smart technologies, portable internet devices, Personal Digital Assistants (PDAs), hand held entertainment systems or portable information technology systems that can be used for word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc

ii. Students may bring their own device for personal use, but they are not permitted to bring a their own device for classroom learning. Our school licencing only covers school owned devices. Thus we may not be able to monitor/filter appropriate material and website access. These devices would not have impero installed, so we would be unable to monitor inappropriate use.

iii. On occasions trainee teachers and visitor may bring their own device and should be given access to the guest wifi only, however, this is a temporary solution. Trainee teachers should be given use of a Perins device as soon as possible.

iv. Any visitor/trainee teacher requesting the guest wifi access must sign the staff AUP which will be located in IT services, a conversation is also important.

v. BYOD will be evaluated with student and staff participation via the ITEL group.

vi. The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, mobile phone or other electronic device until they have a teacher's permission. When abused, the school consequences system will be applied.

vii. Students and parents/guardians participating in BYOD must adhere to the Acceptable User Policy. Additionally, technology:

1. Must be in silent mode while on school campus site.
2. May not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging).
3. May not be used to record, transmit or post photographic images or video of a person, or persons on campus during school activities and/or hours.
4. May only be used to accesses files on computer or internet sites which are relevant to the classroom curriculum. Games are not permitted during lesson time, unless directed by the teacher.

i) **Specialist Software packages**

i. Access to certain software packages and systems such as finance and procurement system, SAP and SIMS will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems

3. Acceptable User Policies

a) AUP – Staff

Perins Staff Acceptable User Policy

This Staff Acceptable User policy forms part of the Perins e-Safety Policy and should be read in conjunction. All staff must agree/sign to confirm their understanding of his policy. If you refuse to sign the declaration, it is still expected that you operate in accordance with the policy and any refusal or failure to operate within the policy may lead to disciplinary action. Where possible staff will accept the policy via Impero. Non-teaching staff will sign upon commencement of their contract. Staff will be reminded of the policy every year.

Unacceptable uses

School systems and resources must not be used under any circumstances for the following purposes.

i. To communicate any information that is confidential to the school or to communicate, share confidential information which you do not have authority to share.
ii. To present personal views and opinions as the views of the school.
iii. To access, view, download, post email or otherwise transmit pornography, sexually suggestive or any other type of offensive, or discriminatory material
iv. To access, view, download, post email or otherwise transmit material that contains viruses.
v. To use the schools facilities to undertake gambling, trading or any other action for personal gain or political purposes.
vi. To undertake any activity which has negative implications for the safeguarding of children and young people.

Any of the above activities (but not limited to) are likely to be regarded as gross misconduct, which may, after proper investigation lead to dismissal. If you are unsure about the use of IT resources including email, advice should be sought from a member of the Senior Leadership Team.

Further Guidance

In addition to the above, please be aware of the following behaviours and act accordingly:

Internet access – All internet activity is subject to monitoring. You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent

access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the Social Media Policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children.

To ensure professional boundaries are maintained, staff should not accept and/or invite the following individuals to be "friends" on personal social media account or other online services unless they can demonstrate that it supports the aims of the school or that there is a family or pre-existing non-School acquaintance:

i. All current students, including vulnerable students who are adults and children
ii. Ex students under the age of 18
iii. Parents/guardians or current students.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device and associated software programmes are password enabled. On no occasion should data concerning personal information be taken offsite without password protection. Staff are reminded to lock their machine when unattended.

Personal Use of School IT – You are allowed to use for personal use however it must conform with the policy restrictions above.

Images and Videos - You should not upload onto any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal IT/Mobile phones - Personal mobile phones are not restricted but should not be used for personal use during lesson time, unless part of your employment, urgent or emergency situations arise. You should consider carefully whether you should share or use your personal mobile phone number when making contact with parents.

Viruses and other malware - any virus outbreaks are to be reported to the IT Services team Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of IT whether you are with other

members of staff or with students.

Cyberbullying - Staff are reminded to keep any records of abuse – texts, emails, voice mails, or instant messages (advise students to do the same). Take screen shots of messages or web pages. Record the time, date and address of the site. Inform the appropriate person Assistant Headteacher or Headteacher, at the earliest opportunity.

Monitoring – The school exercises its right to monitor the use of its IT systems and access or to intercept email and to delete inappropriate materials where it believed unauthorised use of the schools IT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful texts, images or sound.

Agreement

The following agreement will appear on your device via Impero on a yearly basis and a log of all staff will be kept as to who has concurred. If staff do not have regular computer access, other arrangements will be made to ensure that you have read and understood the acceptable use policy and what is expected of you:

I am aware that Internet activity and email communication can be monitored in school and out of school on my school networked device.

I understand that inappropriate use of personal and other non-school based IT facilities can have implications for my employment at Perins where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children.

I understand the school's stance on the use of social networking and given my role working with and around children, will exercise care in any personal use of social networking sites.

I have read and understood the policy, and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of IT facilities, I can seek such clarification from any member of the Senior Leadership Team.

b) AUP - Students

Perins Student Acceptable User Policy

As part of Perins School continued commitment to IT we offer all students supervised access to the Internet and email facilities.

The Internet Service Provider that Perins uses is provided by Hampshire Country Council (www.hants.gov.uk.education). Hampshire offers a heavily filtered service designed specifically for use by schools that allows a very fast and safe Internet connection. Although students are supervised whenever using the internet we cannot guarantee they will not gain access to unsuitable material. We do, however, have an internet monitoring system called 'Impero' which has defined criteria to log any inappropriate websites or keyword violations. If inappropriate material is accessed by students in school, we would ask the student to report the source to staff immediately. We would expect, however, that students do not actively seek such material, as doing so would contravene this agreement and would hold serious consequences including suspension of computer privileges and short term exclusion.

During school teachers will guide students towards appropriate materials and appropriate methods when accessing the internet. Teachers may also use Impero for classroom management, to monitor whether students are on task. Students are given lessons and assemblies about responsibly internet use. Students are expected to abide by the school's code of network etiquette, including:

Student guidelines:

- **Esafety:**
    - Reporting immediately to a member of staff any website or email that contains and unsuitable or inappropriate material.
    - Not revealing your own or anyone else's personal details including home address and phone number
    - I am aware that some people on the Internet are not who they say they are. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
- **Monitoring:** Awareness that internet and emails are monitored for inappropriate activity. Teachers can use monitoring system to check you are on task during a lesson.
- **Email:** Sensible email use with no swearing, vulgarities or inappropriate language. No abusive messages or chain type emails to other users. Manage your email correspondence properly, making sure there is enough space to save your work.
- **Lessons:** Not using the internet or email facilities for personal work or playing games, unless with permission from the teacher.
- **External communication:** Not using the school's name for any electronic correspondence without prior permission
- **Security:** Never use anyone else's username or password, other than your own. Do not access anyone else personal files or disturb anyone else's work. Follow the schools expectations and guidelines when using any networked computer
- **Copyright:** Be aware of copyright rules when copying material from the internet

- **Mobile Devices:** Are to be on silent and not used in lesson unless you have permission from the teacher. You should not take photos or share them without permission.
- **Social networking/Cyberbullying:** Any form of negative or comments behaviour (towards a person or the school) are not acceptable. Students are advised to take screenshots and students will be dealt with according to the school behaviour policy. Students are reminded to keep their privacy and security settings at the highest level.

Signed Student: **Signed Parent:**

4. Training and Curriculum

i. It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Perins School will have an annual programme of training which is suitable to the audience (Appendices 1)

ii. e-Safety for students is embedded into the curriculum; whenever IT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning

iii. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

iv. The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

5. Appendices & Guidance

a. eSafety curriculum (at Nov 2014)

All years	Cyberbullying assembly as part of national anti-bullying week eSafety assembly & responsible internet use (Sept) Tutor activities – Reminder of Student AUP
Year 7	Connect with respect Transform project to coincide with Safer internet day
Year 8	
Year 9	Sexting and dangers of social media
Year 10	Internet exploitation
Year 11	

b. eSafety training programme

Parents	Updates in e-bulletins 2015 - Esafety evening and workshop for parents (oct) 2017 – planned Esafety and cyberbullying / safe2net
Staff	School notebook policy and expectations for notebook usage Responsible internet usage Update on laptop scheme
Staff	Yearly refresher of Acceptable Use Policy acceptance via Impero

6. Risk Assessment & Recording

Key: Likelihood and Impact are between 1 and 3, 1 being the lowest.

Likelihood:	How likely is it that the risk could happen (foreseeability).
Impact:	What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)
Score: (Likelihood x Impact)	**1 – 3 = Low Risk** **4 – 6 = Medium Risk** **7 – 9 = High Risk**

No.	Activity	Risk	Likelihood	Impact	Score	C
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	e- DS Im
1.	Internet browsing/student laptops	Access to inappropriate/illegal content - students	2	3	6	Im
2.	Blogging/social networking	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	