Data Protection Policy

Vita Multi Academy Trust, SO24 9BS

Perins School, Sun Hill Junior School, Perins Pre-School

Contents

Contents

1. Aims

Our organisation aims to ensure that all personal data collected about pupil/students, parents, staff, trustees, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.1. Review and Update Mechanisms

This policy will be reviewed every two years or whenever there are changes to practices or legal requirements to ensure compliance.

2. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

The Trust also complies with the Privacy and Electronic Communications Regulations 2003 (PECR), particularly concerning the use of cookies and similar tracking technologies on its websites, and all forms of electronic direct marketing (e.g., promotional emails or texts to individuals).

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our organisations process personal data relating to parents, pupils/students, staff, trustees, visitors, members and others, and therefore is a data controller.

Vita Multi Academy Trust (the Trust) is registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required. Perins School, Perins Pre-School and Sun Hill Junior School are representatives of the Trust.

5. Roles and responsibilities

This policy applies to all staff and volunteers employed or otherwise engaged by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Members

The Trustee Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations. This responsibility may be delegated to the trust board committees, the CEO and the Headteacher/Head of School/service manager as appropriate.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is contactable via The Data Protection Officer, Vita Multi Academy Trust, c/o Perins School, Pound Hill, Alresford SO24 9BS. Tel: 01962 734361 email: datamanager@perins.hants.sch.uk

5.3 Representatives

The Head Teacher, Head of School of each school and the service manager of Perins Pre-School act as representatives of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns, that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach or potential breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals must seek the prior approval of the DPO before sharing personal data or entering into contracts.

Staff should contact the DPO immediately if they become aware of a breach or potential breach.

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil/student) has freely given clear consent
- "Recognised Legitimate Interests" for specified public interest activities, such as: crime prevention, safeguarding, and responding to emergencies.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and DPA 2018. If we offer online services to pupil/students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil/student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's records retention policy which follows the Information and Records Management Society's guidelines

7.3 Consent

Where we rely on consent as our lawful basis for processing, we will obtain consent from students over 13 years of age. For those under 13, consent for data processing will be obtained from a parent or guardian, with verification of parental responsibility.

7.4 Special Category Personal Data

More strict rules are in place for processing sensitive data like health information, safeguarding concerns, and criminal offence data (e.g., DBS checks). These are all subject to additional security and handling measures.

7.5 Age Appropriate Design

When procuring or designing any online service, educational technology (EdTech) or digital platform likely to be accessed by children, the Trust will apply the principles of the Age Appropriate Design Code and ensure that the best interests of the child are the primary consideration, with privacy and protection set as the default position ('Data Protection by Design and Default')

8. Record of Processing Activities (ROPA)

The ROPA includes:

- the purposes of the processing
- a description of the categories of individuals and of personal data
- the categories of recipients of personal data
- records of consent where this is a lawful basis
- data privacy impact assessment
- details of transfers to third countries, including a record of the transfer mechanism safeguards in place and where the standard of protection in the destination country is **not materially lower** than that in the UK, considering all circumstances. In cases where this is not possible, for example for travel, subjects will be made aware of the risks.
- retention schedules
- a description of the technical and organisational security measures in place.
- The Trust currently does not engage in any solely automated processing that has a legal or similarly significant effect on students or staff. Should the Trust introduce any such solely automated decision-making system, it will ensure that individuals have the right to: (1) be informed that a solely automated decision has been made; (2) make representations about the decision; (3) challenge the decision; and (4) obtain human intervention in respect of the decision

We have an internal record of all processing activities carried out by any processors on behalf of the trust and its schools.

9. Data Protection Impact Assessments

A data protection impact assessment (DPIA) will be undertaken whenever processing of personal information involves:

Systematic and extensive processing:

This includes activities like profiling, especially when decisions based on it have legal or similarly significant effects on individuals.

Large-scale processing of sensitive data:

Processing special category data (like health or biometric data)

Systematic monitoring of public spaces:

Using surveillance technologies or other means to monitor public areas on a large scale.

Use of new technologies:

Introducing new technologies that involve novel forms of data collection and usage, particularly if they pose a high risk to individuals.

Data matching and tracking:

Combining data from multiple sources, tracking individuals' geolocation or behaviour (online or offline), and targeting vulnerable individuals.

Where there's a risk of physical harm:

If a data breach could jeopardize the physical health or safety of individuals.

The DPIA will be completed and measures to reduce risk identified and implemented before processing takes place.

10. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil/student or parent/carer that puts the safety of our students or staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupil/students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils/students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

11. Subject access requests and other rights of individuals

11.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests may be verbal but should be submitted in writing for clarity, either by letter, email or fax to the DPO. They should include:

Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

11.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils/students at our school may not be granted without the express permission of the pupil/student. This is not a rule and pupil/student's ability to understand their rights will always be judged on a case-by-case basis by the Head of School.

11.3 Responding to subject access requests

When responding to requests, the Trust's obligation is to provide the personal data that can be retrieved after a **reasonable and proportionate search** of its records. In addition the Trust:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge, unless there are circumstances to charge a 'reasonable fee' for the administrative costs of complying with a request if:
    - it is manifestly unfounded or excessive; or
    - an individual requests further copies of their data following a request.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil/student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.
- A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

The one-month time limit can be **paused** (the 'stop the clock' rule) if the Trust reasonably requires further information from the requestor to confirm their identity or clarify the scope of the request. The clock will restart once the necessary information is received.

11.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is the basis for processing
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the Trust by contacting the Data Protection Officer or completing the online complaint form here. The Trust will Inform the individual about the outcome of their internal complaint.
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the educational record

Parents, or those with parental responsibility, **do not** have a legal right to free access to their child's educational record (which includes most information about a pupil/student) from academy schools. We will however consider any such request on an individual basis, taking into account circumstances and student wishes. We will respond with a decision within 15 school days of receipt of a written request to the data protection officer. We may charge a fee to provide this information which takes into account administration costs.

13. Biometric recognition systems

Please note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupil/students' biometric data as part of an automated biometric recognition system (for example, pupils/students use face pattern recognition to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parents/carers and pupils/students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils/students. For example, pupils/students can be identified by name and image at the catering point of sale.

Parents/carers and pupils/students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil/student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil/student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

14. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the Surveillance Commissioner's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO in the first instance.

15. Photographs and videos

As part of our school activities, we may take photographs and record images/video of individuals within our school. We will obtain written consent from parents/carers, or pupils/students aged 13 and over, for photographs and videos to be taken of pupils/students for communication, marketing and promotional materials. This will be requested annually via a school data collection.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil/student. Where we don't need parental consent, we will clearly explain to the pupil/student how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school newsletters, brochures, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further if it is already in the public domain.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See the schools' Child Protection, Safeguarding and Social Media Policies for more information on our use of photographs and videos.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing

activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

17. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain
- personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staff workroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils/students are reminded to change their passwords at regular intervals. Multi factor authentication will be enabled wherever possible.
- Disk encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils/students or trustees who have explicit permission to store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our e-safety Policy and local IT Acceptable Use Policy (Staff))
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- The Trust adheres to the DfE Cyber Security Standards for schools. This means the Trust ensures minimum standards are met for
    - Boundary firewalls and internet gateways.
    - Secure configuration.
    - Access control.
    - Malware protection.
    - Patch management.

18. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and meets ISO27001/27002.

19. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils/students eligible for the pupil/student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a non-encrypted school laptop containing non-encrypted personal data about pupils/students

20. Training

All staff (including volunteers and trainees) and trustees are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every 2 years and shared with the trust board.

22. Perins School Archive

A Perins School archive is maintained as a resource to help inspire and equip current staff and students to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations of alumni; and to serve as a research resource for all interested in the history of Perins School and the community it serves.

23. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme

- IT Acceptable Use Policy (Staff)
- Child Protection policy
- Safeguarding policy
- Social Media policy
- Online safety policy
- CCTV policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher/head of school, CEO and the chair of trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Trust's online software platform, 'GDPR Sentry'.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more
- robust processes or providing further training for individuals)
- Records of all breaches will be stored in the individual school's 'GDPR Sentry' online software platform.
- The DPO and CEO, head teacher/head of school/service manager will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. To mitigate against such an error- all such email recipients should be checked by a suitably authorised colleague.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

In any cases where the recall is unsuccessful, the DPO will ask the sender to contact the relevant unauthorized individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search within 10 working days to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that could occur include:

- Details of pupil/student premium interventions for named children being published on the school website
- All published information should be checked by at least two members of staff prior to publication or upload.
- Non-anonymised pupil/student exam results or staff pay information being shared with trustees
- All information for external publication should be checked by a Senior Leader prior to publication. All information for Trustees and Trustees should be checked by the Governance Professional prior to distribution.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- All school devices should be encrypted using Bit Locker as a minimum level of security. Appropriate measures should be in place and regularly tested and reviewed to minimise

the possibility of malicious hacking. All staff should adhere to the data security measures detailed in the acceptable use of IT and personal data handling policies.

- The school's cashless payment provider being hacked and parents' financial details stolen

Vita Multi Academy Trust undertakes to only use data processors who are able to demonstrate compliance with data protection legislation. Should a breach occur, it would be reported in the normal way, but the data processor will have a similar duty to take appropriate measures, including reporting any such breach and informing those whose data has been compromised.