Presdales School

Title	Data Protection Policy
Version	April 2018
Author/Title	Margaret Stanley, Business Manager
Committee Responsible	Students
Governor Link	Oyinda Bishi
Date approved by Committee	November 2018
Date approved by Full Governing Body	NA
Review Date	Summer term 2: 2019

Enquiries & comments
Any enquiries and comments about this publication may be made to:

Telephone: 01920 462210 / **Email:** admin@presdales.herts.sch.uk
Address: Hoe Lane, Ware, Hertfordshire SG12 9NX

Contents

1. Aims

During the course of its activities Presdales School Academy Trust will process personal information about a number of different groups of people, all of which have rights with regard to how their personal data is handled. The Trust aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in an appropriate and lawful manner and in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

The objective of the policy is to ensure that the Trust and its trustees, members and employees are informed about and comply with their obligations. This policy meets the requirements of the GDPR and the expected provisions of the 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. In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Biometric Data	Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allow or confirm the unique ID of the person, such as facial images, finger scans.
Consent	Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or clear affirmative action signifies agreement to the processing of Personal Data relating to him or her.
Data	Data is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV. Such information is subject to certain legal safeguards specified in GDPR and other legislation. GDPR imposes restrictions on how the information may be used.
Data Subject	The identified or identifiable individual whose personal data is held or processed, including, job applicants; current, past and prospective employees, students and parents/carers/other family members; trustees;
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Users	Includes employees, volunteers, trustees, whose work involves using personal data. Data users have a duty to protect the information they handle by following the Trust's data protection and security policies at all times.
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.
Parent	Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child
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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. It can be automated or manual
Sensitive personal data	Personal data which is more sensitive and thus 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

4. The data controller

Presdales School is a Single Academy Trust which processes personal data relating to parents, students, staff, trustees, visitors and others. The Trust is therefore a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by the school, and to external organisations or individuals working on its behalf. Members of staff who do not comply with this policy may face disciplinary action.

5.1 Board of Trustees

The Board has overall responsibility for ensuring that the school complies with all relevant data protection obligations. The Board approves the Data Protection Policy which sets out the procedures for obtaining, handling, processing, storing, transportation and destruction of personal information. Trustees are also likely to process Personal data whilst performing their duties

5.2 Data protection officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the school's compliance with data protection law, and developing related policies and guidelines to ensure that the essential aspects of the GDPR are embedded into the Trust's culture and that operations adequately safeguard Personal Data.

The DPO should be provided with necessary support and resources to effectively carry out their tasks including support from management, time to fulfill their duties, adequate resources, access to support services and training. The DPO must be able to carry out the role independently without the influence of other personnel.

The DPO reports directly to the Board of Trustees. An annual report will be submitted to the Board and where necessary the DPO will advise and make recommendations to the Board on data protection issues

The Trust's DPO is Mrs J Stephenson (Deputy Headteacher) who is contactable via email on DPO@presdales.herts.sch.uk. There is also an assigned link governor who has an overview of the GDPR procedure in our organization. This post is held by Mrs Oyinda Bishi.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

5.3 Headteacher

The Headteacher acts as the representative 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 own 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
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that the 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 and processing personal data

7.1 Lawfulness, fairness and transparency

The GDPR is not intended to prevent the processing of personal data but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Trust will only process personal data under 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 student) has freely given clear **consent**

7.1.1 Consent is required in certain circumstances including, but not limited to, the use of students' photographs on the school website, school prospectus or social media, and before students are signed up to online services.

- A Data subject must 'consent' to processing of their personal data by a statement or positive action. Consent requires affirmative action so silence, inactivity or pre-ticked boxes are unlikely to be sufficient.
- Where a student is less than 13 years of age consent is obtained from parents/carers (except for online counselling and preventive services). Once students reach the age of 13 they are responsible for their own data and the consent of the student will be required in some circumstances, although the Trust will consider whether it is appropriate to inform parents about this process.
- Data subjects must be easily able to withdraw consent at any time.
- Evidence and records of consent must be maintained so that the Trust can demonstrate compliance with consent requirements.

7.1.2 Privacy Notices

The Trust has developed privacy notices which will be issued to students, parents/carers, staff and trustees. Privacy notices will be concise, transparent, intelligible and easily accessible. They will be written in clear and plain language, particularly for students and free of charge.

7.1.3 Sensitive personal data

The Trust will be processing Sensitive Personal Data and recognises that the law states that this type of Data needs more protection. As well as establishing a lawful basis, the Trust will meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. These include:

- Data Subjects explicit consent having been received
- Processing is necessary for reasons of substantial public interest

- Processing is necessary for the purposes of carrying out the obligations or exercising specific rights of the Data Controller or Subject in employment law
- Processing is necessary to protect the vital interests of the Data Subject or another where the Data Subject is incapable of giving consent

Unless another legal basis for processing is applicable, explicit consent is usually required for processing sensitive personal data. Appropriate safeguards must also be in place when processing confidential data such as details of family circumstances, child protection or safeguarding issues.

7.1.4 Confidential data

The Trust is also likely to process data which is confidential in nature such as family circumstances, child protection or safeguarding issues and appropriate safeguards must be implemented even if this information does not meet the legal definition of sensitive personal data.

7.1.5 Criminal Convictions and offences

There are separate safeguards in the GDPR for personal data relating to criminal convictions or offences. Such data may be processed as part of pre-employment vetting checks on employees or trustees or occasionally acquired regarding students and parents/carers. Where appropriate and when lawful to do so, such information may be shared with external agencies

7.2 Limitations and Controls

- The Trust 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. The Trust will ensure that Personal Data collected is adequate to carry out its functions and that the information is relevant to the intended purposes and limited to what is necessary.
- If the Trust wishes to use personal data for reasons other than those given when it was first obtained, the individuals concerned will be informed in advance, and consent obtained where necessary.
- The Trust will implement measures to ensure the security of data held in any format.
- Staff must only process personal data where it is necessary in order to carry out their roles and access is restricted on a 'Need to Know' basis.
- Trustees are likely to process personal data whilst performing their duties and must ensure that data is they adhere to the Trust's data protection policies and be informed about their responsibilities to keep data secure. This includes keeping data secure from third parties, using a designated Trust email account, ensuring that electronic Trust-related communication and information is encrypted and that hard copy documents are securely stored.
- Personal data must be accurate, relevant and kept up to date and the Trust will take steps to ensure that it is checked regularly
- Personal data held in any format should not be kept longer than necessary for the purpose for which it is held. When the personal data is no longer needed for specified purposes it must be deleted or anonymized, in accordance with the guidance contained in Information and Records Management Society's toolkit for schools and the school's Data Retention Policy
- The Trust has put in place appropriate measures to prevent unlawful or unauthorized processing of personal data and accidental loss of or damage to personal data. Personal data in all formats must be stored securely from the point of collection to the point of disposal.

8. Sharing personal data

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

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- The school needs to liaise with other agencies – we will seek consent as necessary before doing this
- Suppliers or contractors need data to enable us to provide services to our staff and 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 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.

The trust may share personal data with the following third parties where it is lawful and appropriate to do so including, but not limited to:

- Local Authorities
- The Department for Education
- The Education and Skills Funding Agency
- The Disclosure and Barring Service
- The Teaching Regulation Agency
- The Teachers' Pension Service
- The Local Government Pension Scheme
- Serco external HR and Payroll provider
- HMRC
- Police and other law enforcement agencies
- Legal advisors and other consultants

- Occupational Health Services
- NHS professionals including educational psychologists and school nurses
- Education Welfare Officers
- Courts, if ordered to do so
- Prevent teams in accordance with the Prevent Duty on schools
- Other schools, eg if negotiating a managed move and we have consent to share information in these circumstances
- Confidential waste collection companies
- Examination boards
- Joint Council for Qualifications

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Data subjects have rights of access to their own personal data and may 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 must be submitted in writing, 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.

9.2 Students 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 12 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

students at the school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request, in which case most requests may be granted without the express permission of the student.

9.3 Responding to subject access requests

When responding to requests, we:

- 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
- 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 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.

9.4 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
- 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 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. The identity of an individual requesting data must be verified.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, will be given access to their child's educational record (which includes most information about the student) within 15 days school days of receipt of a written request.

11 Biometric Data

The Trust processes Students' biometric data as part of an automated biometric recognition system (for example, for cashless catering and sixth form registration processes) and complies 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 obtain written consent from at least one parent or carer before any biometric data is collected from their child and first processed. (Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.)

Parents/carers and students have the right to choose not to use the school's biometric systems. Alternative means of accessing the relevant services will be provided for those students.

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

As required by law, if a 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 student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), their consent will be obtained 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.

12 CCTV

The school does not currently use CCTV

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

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

Uses may include:

- Within school on notice boards, in the school prospectus and newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- Online on our school website or social media pages
- Prospectus

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.

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

See our Online Safety policy for more information on our use of photographs and videos.

14. Data protection by design and default

The school will put measures in place to show that data protection has been integrated 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 **data 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

15. Data security and storage of records

The school 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 staffroom 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 students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safety Policy/acceptable use agreement)
- 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)

16. 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.

17. Personal data breaches

The school 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 students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

18. Training

All staff and governors 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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Board of Trustees.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection Policy
- Online Safety Policy
- Data Retention 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 and the chair of governors
- 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 on the school network in the GDPR file.
- 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 on the school network in the GDPR

  The DPO and headteacher 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*
- *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 contact the relevant unauthorised 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 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 you might want to consider could include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised student exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*