Data Protection & GDPR Policy

Policy Title: Data Protection & GDPR Policy

Version: 1.0

Date: July 2025

Review Date: July 2026

Owner: Executive Headteacher

Approval: Governing Board

Contents:

1. Introduction and purpose

1.1 This policy sets out the school's commitment to handling personal data in line with the General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (collectively referred to as the data protection legislation).

1.2 The school is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number (ZA001361). Details about this registration can be found at www.ico.org.uk

1.3 The purpose of this policy is to explain how the Apollo Education handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the school's behalf, of the school's expectations in this regard.

2. Scope

2.1 This policy applies to the processing of personal data held by the school. This includes personal data held about pupils, parents/carers, employees, temporary staff, governors, visitors and any other identifiable data subjects.

2.2 This policy stipulates the following procedures and documentation, which refer to the handling of personal data, shall be maintained:

- Personal Data Breach Handling Procedure
- Data Protection Request Handling Procedure
- Record Retention Schedule

3. Definitions & Legislation

3.1 There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the school. These are:

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.

3.2 Relevant Legislation

This policy is informed by the following legislation:

- UK General Data Protection Regulation (UK GDPR), 2021
- Data Protection Act 2018
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Keeping Children Safe In Education 2025
- DfE Data Protection guidance

4 Data Controller & Roles and Responsibilities

4.1 Data Contoller

Apollo Education processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. Apollo Education is registered as a data controller with the ICO (Reg. No. INSERT) and will renew this registration annually or as otherwise legally required.

4.1 Governing Board

The Governing has overall responsibility for ensuring the school implements this policy and continues to demonstrate compliance with the data protection legislation (as the Data Controller representative). This policy shall be reviewed by the Governing Board on an annual basis.

4.2 Executive Headteacher

The Executive Headteacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the school's behalf.

4.4 Data Protection Officer

Appointed by the Executive Headteacher, the Data Protection Officer (DPO) is responsible for carrying out the following tasks:

- Informing and advising the school of their obligations under the data protection legislation
- Monitoring compliance with data protection policies
- Raising awareness and providing training
- Carrying out audits on the school's processing activities
- Providing advice regarding Data Protection Impact Assessments and monitoring performance
- Co-operating with the Information Commissioner's Office
- Acting as the contact point for data subjects exercising their rights

4.5 Employees, temporary staff, contractors, visitors

All employees, temporary staff, contractors, visitors and others processing personal data on behalf of the school, are responsible for complying with the contents of this policy. Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

4.6 All employees, temporary staff, contractors, visitors shall remain subject to the common law duty of confidentiality when their employment or relationship with the school ends. This does not affect an individual's rights in relation to whistleblowing. On termination of employment, employees shall return all information and equipment to the school, including personal identification passes/smart cards and keys.

4.7 Unauthorised access, use, sharing or procuring of the school's data may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

4.8 Employees shall have no expectation of privacy in their use of the school's systems. Any correspondence, documents, records or handwritten notes created for work related purposes, may be disclosable to data subjects or the public under the UK General Data Protection Regulation.

4.9 The school reserves the right to monitor employees' use of the school's systems and where necessary access work related emails and messages sent from work accounts. This may be done without notice. Employee monitoring and access to data will only be carried out where this is considered necessary and proportionate, for example to discharge the school's statutory duties in relation to safeguarding, health and safety, statutory reporting and responding to information requests. It may also be carried out for security purposes, to identify suspicious activity, compliance with school policies, quality checking and training purposes.

5 Data protection by design and by default

5.1 The school is committed to ensuring that data protection considerations are at the heart of everything it does involving personal data, and shall ensure that it has appropriate technical and organisational measures in place which are designed to implement the Data Protection Principles in an effective manner.

5.2 The school shall ensure that by default, it will only process personal data where it is necessary to do so, and appropriate safeguards are in place to protect it. This Data Protection Policy and supplementary policies, procedures and guides demonstrate how the school achieves their 'data protection by design and default' obligations.

6 Data Protection Principles

6.1 The UK GDPR provides a set of 6 principles which govern how the school handles personal data. These are set out in Article 5 of the UK GDPR, 2021. All employees, temporary staff, contractors, and other individuals processing personal data on behalf of the school are responsible for complying with the data protection principles:

6.2 Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

6.3 This means personal data shall only be processed where there is a lawful basis which allows this; we are fair to data subjects when we use or share their personal data (ie we must act in a way they would reasonably expect); and are transparent in how we handle personal data by describing this in our privacy notices.

6.4 The data protection legislation lists the different lawful bases which permit the collection, use and sharing etc of personal data. These are contained in Article 6 of the UK GDPR. At least one of these legal bases must apply when processing personal data. In summary:

- The data subject has given consent.
- It is necessary for contractual purposes.
- It is necessary to comply with a legal obligation.
- It is necessary to protect someone's life.
- It is necessary to carry out a task in the public interest or exercise our official duties.
- It is necessary to pursue the school's legitimate interests or a third party's legitimate interests, except where such interests are overridden by the data subject, in particular, where the data subject is a child.

6.5 When 'special categories' of personal data are processed (ie data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent.
- The processing is necessary for employment, social security or social protection purposes(e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud).

- It is necessary to protect the data subject's life and they are physically or legally incapable of giving consent.
- The data subject has made the information public
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest and are proportionate to the aim pursued.
- The processing is necessary for health or social care purposes.
- The processing is necessary for reasons of public interest in public health.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes

6.6 Although consent is one of the lawful bases that can be relied upon when processing personal data or special category data, it is not appropriate to rely on this for most of the processing the school does. This is because there is a high standard for achieving 'valid' consent and there are potential difficulties for the school should the data subject later withdraw their consent to the processing. The school shall therefore look for alternative lawful bases to legitimise its processing where they are more appropriate, such as 'processing is necessary to carry out a task in the public interest' and 'processing is necessary for the purposes of employment, social security or social protection'.

6.7 There are however circumstances when the school is required to obtain consent to process personal data, for example:

- To collect and use biometric information (eg fingerprints and facial images) to be used for identification purposes.
- To send direct marketing or fundraising information by email or text, where the data subject would not have a reasonable expectation that their data would be used in this way or has previously objected to this.
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena (such as on social media, on the school website; in the Press; in the prospectus; newsletter etc), where the data subject would not have a reasonable expectation that their images would be used in this way, or the rights of the data subject override the legitimate interests of the school.
- To share personal data with third parties (e.g. professionals, agencies or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

6.8 Where it is appropriate for the school to use consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent.

6.9 Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned. Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child reaches their 13th birthday. Consent shall be obtained directly from children aged 13 years and over where those children are deemed by the school to have sufficient maturity to

make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).

6.10 The school shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw or amend their consent, and instructions on how to do this easily.

6.11 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').

6.12 This means the school shall only collect and use personal data for the reasons specified or described in its privacy notices and shall not process this data in any way which could be considered incompatible with those purposes, in other words, using the data for a different or unexpected purpose.

6.13 Personal data shall be adequate, relevant and limited to what is necessary for the purpose it was processed ('data minimisation').

6.14 This means the school shall ensure that any personal data collected, used or shared etc. is fit for purpose, relevant and not excessive or disproportionate for the purpose it was intended.

6.15 Personal data shall be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay ('accuracy').

6.16 This means the school shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date, and where personal data is found to be inaccurate, this information shall be corrected or erased without delay.

6.17 The school shall send reminders, on at least an annual basis, to parents/carers, pupils and employees, asking them to notify the school of any changes to their contact details or other information. The school shall also carry out periodic sample checks of pupil and employee files to ensure the data is accurate and up to date.

6.18 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed ('storage limitation).

6.19 This means the school shall not keep personal data for any longer than it needs to. Personal data may be stored for longer periods where it is solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the data subject.

6.20 The school shall maintain and follow a Record Retention Schedule which sets out the timeframes for retaining and disposing of personal data.

6.21 The school shall designate responsibility for record retention and disposal to data leads, who shall adhere to the school's Record Retention Schedule and ensure the timely and secure disposal of the data.

6.22 Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (‘integrity and confidentiality)

6.23 This means the school shall have appropriate security in place to protect personal data. The following are examples of the minimum technical and organisational measures that shall be in place to protect personal data:

6.24 Technical security measures include:

- Security patches shall be applied promptly.
- Access to systems shall be restricted according to role-based requirements.
- Strong password policies shall be enforced; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others. Password managers shall be utilised where possible
- Portable devices (such as laptops) and removable media (such as USBs) storing personal data shall be encrypted.
- Data shall be backed up regularly.
- The school’s disaster recovery and business continuity plans shall be regularly tested to ensure data can be restored in a timely manner in the event of an incident.
- Two factor authentication (2FA) shall be enabled on systems containing sensitive data.

6.25 Organisational security measures:

- Employees shall sign confidentiality clauses as part of their employment contract.
- Mandatory data protection awareness training shall be provided to employees and governors during on-boarding and annually thereafter.
- Cyber security training, guidance or advice shall be cascaded to employees on a regular basis.
- Policies and guidance shall be communicated to employees and governors on the secure handling of personal data in school and when working remotely.
- Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings. All employees shall be given the opportunity to raise compliance queries or concerns at any meeting.
- Cross cutting shredders and/or confidential waste containers will be available on the school’s premises and used to dispose of paperwork containing personal data.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying confidential paperwork off school premises.
- The school’s buildings, offices and where appropriate classrooms, shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.
- Procedures shall be in place for visitors coming onto the school’s premises. These will include signing in and out at reception, wearing a visitor’s badge and being escorted where appropriate.
- The school shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.
- The school shall have procedures in place to effectively wipe all data from redundant computer equipment (to include smartphones, tablets, cameras, memory cards,

photocopiers, multi-function devices, CDs, USBs etc) prior to their decommissioning, re-use or disposal. The equipment shall be stored in a secure area pending their collection by disposal companies.

6.26 The school shall have appropriate records in place to demonstrate compliance with each of these data protection principles ('accountability').

7 Data subjects' rights

7.1 Data subjects have several rights under the data protection legislation. The right to:

- be told how their personal data is being processed;
- request access to their personal data;
- request that inaccurate or incomplete personal data is rectified;
- request the erasure of personal data in certain circumstances;
- request the processing of their personal data is restricted in some circumstances;
- request that their personal data is transferred from one organisation to another or given to them, in certain circumstances;
- object to their personal data being used for public interest or direct marketing purposes;
- prevent important decisions being made about them by solely automated means (including profiling);
- complain to the school about the handling of their personal data. If they remain dissatisfied with school's response, they have the right to escalate this to the Information Commissioner's Office.

7.2 Data subjects may exercise their data protection rights by contacting the school in writing or verbally. Data subjects are recommended to submit their request in writing and send this to Executive Headteacher, Apollo Education.

8 Personal data breaches

8.1 The school shall follow the Personal Data Breach Handling Procedure in the event of a personal data breach. A personal data breach is a: 'breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'.

8.2 Examples of personal data breaches include, but are not limited to:

- Emailing a group of parents and failing to insert their private email addresses into the 'Bcc' field, thus revealing those email addresses to all recipients.
- Emailing or posting confidential information to the wrong person.
- Not storing or disposing of confidential paperwork securely.
- Loss or theft of IT equipment which has personal data stored on it eg a laptop, iPad, mobile phone or a USB.
- Altering, sharing or destroying personal data records without permission from the school.
- Using another person's login credentials to gain higher level access to records.
- Sharing login details or having insufficient access controls to systems, which result in unauthorised viewing, use, modification or sharing of personal data.
- Hacking into a system containing personal data.

- A social engineering incident whereby a person uses deception to manipulate individuals into divulging confidential or personal information eg a phishing email.
- A cyber-attack resulting in loss of access to personal data (eg a ransomware attack).
- Environmental incidents such as a fire or flood which damage or destroy important personal data records, prior to their scheduled disposal.
- An employee abusing their access privileges to look at someone else's records out of personal curiosity or gain.

8.3 All personal data breaches and suspected breaches (including cyber incidents) shall be reported to the Data Protection Officer immediately

8.4 All incidents shall be recorded on the school's personal data breach log and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Data Protection Officer.

8.5 Notification to the ICO and Data Subjects: The Data Protection Officer shall determine whether the school must notify the Information Commissioner's Office and data subjects following a personal data breach. A personal data breach is required to be reported to the ICO within 72hrs of the school becoming aware of the breach, where the breach is likely to result in a risk to the data subject or someone else, for example if they are likely to suffer damage, discrimination, disadvantage or distress.

8.6 Data subjects are required to be informed without undue delay, where the breach is likely to result in 'high risks', for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm. The Data Protection Officer shall notify the ICO (following consultation with the school) where a personal data breach meets the 'risk' threshold. The Headteacher or other delegated employee shall notify data subjects (or their parents) following a 'high risk' breach.

9. Sharing Data

9.1 The school regularly shares personal data internally and externally with partner agencies and third parties for legitimate purposes. Employees shall follow to the school's policies and procedures when sharing personal data and adhere to the statutory and non-statutory guidance as set out in the:

- HM Government: Information Sharing Advice for Safeguarding Practitioners (2023)
- Department for Education: Keeping Children Safe in Education (2024)
- Information Commissioner Office: Data Sharing Code of Practice (2021)

9.2 When sharing personal data with third parties the school shall adhere to the following principles:

- Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing.
- An appropriate lawful basis shall be identified prior to the sharing.
- Data shared shall be adequate, relevant and limited to what is necessary.
- Accuracy of the data shall be checked prior to the sharing (where possible).
- Expectations regarding data retention shall be communicated.

- Data shall be shared by secure means and measures in place to protect the data when received by the third party.
- A record shall be kept of the data sharing.
- Information sharing agreements shall be in place where required.

9.3 The school understands the data protection laws expressly allow organisations to share necessary and proportionate personal data with third parties to protect the safety or well-being of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm, and is not a barrier to sensible and necessary sharing

9.4 Sharing data with suppliers (data processors) The school uses a variety of service providers to help it run effectively. These are sometimes referred to as 'data processors'. This often includes companies providing services such as IT support, professional advice, learning or teaching resources, management information systems, parent communication platforms, document storage solutions, Artificial Intelligence platforms, visitor entry systems, facial recognition and biometric data storage systems, HR and payroll platforms.

9.5 Using these service providers usually requires disclosing personal data to them so they can deliver the service or product the school has purchased or subscribed to. The data protection legislation requires that before sharing personal data with a service provider, the school must carry out due diligence checks on the company or product, to assess they have appropriate measures in place that ensures compliance with the data protection legislation and protects the rights of data subjects.

9.6 Due diligence checks shall be carried out on prospective service suppliers by the school, alongside the Data Protection Officer prior to using the service or product provided by the supplier. The outcome shall be recorded on the school's Data Processor Due Diligence Report template.

9.7 Employees shall not purchase a product or service which involves the disclosure of personal data, unless the appropriate due diligence checks have been carried out in consultation with the Data Protection Officer, a data processing agreement is in place, and the product has been approved by a member of SLT (or other delegated person).

10 Data Protection Impact Assessments

10.1 The school is required to carry out Data Protection Impact Assessment (DPIAs) on the processing of personal data, where this is likely to result in 'high risks' to the rights and freedoms of data subjects. High risk means the potential for any significant physical, material or nonmaterial harm (eg distress) to individuals.

10.2 A DPIA is a process which helps the school identify, minimise and document the data protection risks of a project or plan involving personal data. It demonstrates the school's compliance with the data protection principles and fulfils its 'accountability' and 'data protection by design' obligations. A DPIA does not have to eradicate all risk, but should minimise risks and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what the school wants to achieve.

10.3 The UK GDPR sets out three types of processing which will always require a DPIA:

- Systematic and extensive evaluation or profiling of individuals with significant effects
- Large scale use of sensitive data (special category or criminal conviction or offence data)
- Systematic monitoring of a publicly accessible area on a large scale

10.4 The school shall follow the Information Commissioner's Office supplementary list of processing, which also requires a DPIA:

- Use of innovative technology (including the use of Artificial Intelligence (AI))
- Denial of a service, opportunity or benefit
- Large scale profiling
- Processing of biometric or genetic data
- Data matching
- Invisible processing
- Tracking
- Targeting children or other vulnerable individuals
- Risk of physical harm

10.5 The school shall also consider the European guidelines (Guidelines on Data Protection Impact Assessment), to help identify other likely high risk processing, which includes:

- Use of sensitive data or data of a highly personal nature.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.

10.6 The school shall use their DPIA pre-screening checklist to help identify whether a DPIA should be carried out. The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA to ensure the mitigations are put in place. DPIAs shall be reviewed on an annual basis

11 Records management

11.1 Records management is a system for managing records throughout their life cycle, from the time of creation or receipt to their destruction. The school recognises that good records management plays a crucial role in the smooth running of the school and is also necessary to comply with its obligations under the data protection legislation and the Freedom of Information Act 2000, particularly when responding to information access requests and protecting personal data from security threats.

11.2 The school shall manage its electronic and paper-based records in line with the statutory Code of Practice on the Management of Records, issued under section 46 of the Freedom of Information Act 2000.

11.3 Employees and governors shall be provided with advice, guidance and training on how to manage the school's records effectively throughout their lifecycle. This should include naming, storing, accessing, security classification, and disposal of records.

11.4 The school shall maintain a record retention schedule and regularly review its records to ensure they are disposed of in line with the schedule. The schedule shall be communicated to data leads responsible for managing the school's records.

11.6 The school shall, amongst other things, know what personal data records it holds, who it shares these records with; the security in place to protect them and how long they are to be kept for. This information shall be recorded in a Record of Processing Activities Inventory (ROPA), in line with Article 30 of the UK GDPR. The ROPA shall be reviewed annually and made available to the Information Commissioner upon request.

12. Training

12.1 All staff and governors are to be 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.

13. Monitoring arrangements

13.1 The DPO is responsible for monitoring and reviewing this policy.

13.2 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 governing board.

Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the UK GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.

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 Co-Headteachers and the Co-Chairs 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 securely on the school's computer system
- 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 securely on the school's computer system.
- The DPO and Co-Headteachers 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