Policy No: 5(A).1

LIFE SCHOOL

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY AND PROCEDURES

This policy, which applies to the whole school, is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from school office or Designated Safeguarding Lead.

Document Details

Information Sharing Category	Public Domain
Version	V1
Date Published	01/01/2021
Authorised by (if required)	Chief Executive Officer
Review / Update Date	01/01/2022
Responsible Area	Proprietor and Senior leadership team

Amendments:

Date	Amendment

Availability: This policy applies to all activities undertaken by the school, inclusive of those outside of the normal school hours and away from the school site and is inclusive of all staff (teaching, support and agency staff), students on placement, contractors, the Chief Executive Officer, the Advisory Board and volunteers working in the school. All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy being required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the *Policies Register.*

Monitoring and review:

- This document will be subject to continuous monitoring, refinement and audit by the Headteacher
- This policy was last reviewed agreed by the Advisory Board in January 2021 and will next be reviewed no later than January 2022 or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed:

Sarah Quilty
Headteacher

Alastair Saverimutto
Chief Executive Officer

Contents

Aims:

Our school aims to ensure that all personal data collected about staff, pupils, parents, the chief executive officer, visitors and other individuals is collected, stored and processed 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.

Legislation and guidance

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.

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

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

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. In our case this is the chief executive officer.
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.

The data controller

LIFE SCHOOL processes personal data relating to parents, pupils, staff, Chief executive officer, visitors and others, and therefore is a data controller.

The school, through our Chief executive officer, is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The school's registration number is INSERT REGISTRATION NUMBER.

Roles and responsibilities

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

Chief executive officer

The Chief executive officer ensures that our school complies with all relevant data protection obligations.

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. In LIFE SCHOOL the DPO is INSERT NAME AND APPOINTMENT.

- The DPO will provide an annual report of their activities to the Board of Chief executive officer in the summer term 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.
- Details of the DPO's responsibilities are set out in their job description. The Headteacher acts as the representative of the data controller on a day-to-day basis.

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 – see LIFE SCHOOL Data Breach Procedure
  - 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

Data protection principles

The 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.

Collecting personal data

What data we collect:

We collect and hold personal data and information relating to our staff and students directly from their Student(s)/guardian(s) at the time of application to register and joining the School and may also receive information about

them from their previous School, local authority and/or the Department for Education (DfE). We also create personal information about the student during their time in the School in the form of assessments, marking of work and reports.

The categories of information that we collect, hold and share include:

- personal information (such as name, unique student number and address);
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- attendance information (such as sessions attended, number of absences and absence reasons);
- relevant medical, special education needs (SEN) and mental health information;
- exclusions/behavioural information;
- photographs: We collect photographic images of our staff and students, which we use for purposes of identification and also for marketing purposes;
- CCTV: images of staff, faculty members, parents, students and other visitors to the School will be captured by our CCTV system which monitors public areas including the main entrance used by visitors, the pedestrian and vehicle gates, and the entrances to all other School buildings;
- disclosure and Barring Service Information (for adults working within the school) and
- Internet search history/usage.

Why we collect and use this information: We process personal information to enable us to provide education and training conducted outside the State system, welfare and educational support services, to administer school property and library services, to maintain our own accounts and records, for administration in connection with boarding and the organisation of alumni associations and events, for fundraising purposes, to ensure physical security of the School and its assets and to support and manage our staff. The information we process that is relevant to the above reasons/purposes include:

- personal details
- family details
- lifestyle and social circumstances
- financial details
- education and employment details
- disciplinary and attendance records
- visa-related checks and references from previous schools
- visual images, personal appearance and behaviour
- details of goods and services provided

We also process sensitive classes of information that may include:

- physical or mental health details
- sexual life
- racial or ethnic origin
- religious or other beliefs
- information relating to offences or alleged offences

Collecting information: Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation (GDPR), we will inform you whether you are required to provide certain student information to us or if you have a choice in this and, where necessary, seek your consent for us to use that data and information in the way we intend.

How we use student information: We use this personal data:

- for the purposes of student assessment and to confirm the identity of prospective students and their parents;
- to provide education services (including SEN), career services, and extra-curricular activities to students; monitoring students' progress and educational needs; and maintaining relationships with alumni and the School community;
- for the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the School's performance;

- to give and receive information and references about past, current and prospective students, including relating to outstanding fees or payment history, to/from any educational institution that the student attended or where it is proposed they attend;
- to enable students to take part in national or other assessments, and to publish the results of public examinations or other achievements of students of the School;
- to safeguard students' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips;
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's E-Safety Policy; to make use of photographic images of students for identification purposes and in School publications, on the School website and (where appropriate) on the School's social media channels, where parental permission has been given, and in accordance with the School's E-Safety Policy;
- for security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and
- where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

We may keep details of addresses when children leave the School so we can send you news about the School.

We may use information about you if we need this for historical research purposes or for statistical purposes, with such information being anonymised/pseudonymised.

Who we share student information with: In accordance with our legal obligations, we may share information with local authorities, the Independent Schools Inspectorate and the Department for Education, for example, where we have any safeguarding concerns. Other instances where we may share information include:

- On occasion, we may need to share information with the police and other authorities, such as social services
- We may also need to share information with our legal advisers for the purpose of obtaining legal advice.
- Occasionally we may use consultants, experts and other advisors to assist the School in fulfilling its obligations and to help run the School properly. We might need to share your information with them if this is relevant to their work.
- If your child is not of British nationality we have to make sure that your child has the right to study in the UK. We might have to provide information about you to UK Visas and Immigration to comply with our duties as a Tier 4 sponsor.
- We may share some information with our insurance company, for example, where there is a serious incident at the School.
- If you have unpaid fees while your child is at the School we may share information about this with other schools or educational establishments to which you intend to send your child.
- If your child leaves us to attend another school we may need to provide that school with information about you. For example, details of family circumstances for safeguarding reasons.
- We may share information about you with others in your family, such as another parent or step-parent. For example, where this is part of our obligation to take care of your child, as part of our wider legal and regulatory obligations, or in connection with school fees.
- We may need to share information if there is an emergency, for example, if you are hurt whilst on School premises.

  We do not share information about our students with anyone without consent unless the law and our policies require or allow us to do so.

How we use parent information

We collect and process personal data relating to the parents of students at the School. This is for contractual purposes and/or to enable the payment of fees. This personal data includes identifiers such as names, addresses, email addresses and telephone numbers, characteristics such as ethnic group and financial information such as credit card/banking details. Upon accepting an offer of a place at the School for your child, you will have been offered an opportunity to consent or otherwise to our sharing your contact information with other parents in your child's cohort. The purpose of this sharing of information is to facilitate the wider School community including the promotion of fundraising efforts. We will not share your contact information unless explicit consent has been given.

Consent for the sharing of your data in this way may be given or withdrawn by you at any time during your child's attendance at the School. If you wish to change your consent please contact the school at INSERT SCHOOL EMAIL ADDRESS.

We will not share information about you with third parties without your consent unless the law or our policies require or allow us to do so. We are required, by law to pass on some of this personal data to:

- our local authority
- the Department for Education (DfE)

- 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 licensed body, 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) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. If we offer online services to pupils, such as classroom apps which require use of personal data, and we intend to rely on consent as a basis for processing, we will get parental consent as our pupils are under 13. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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 and through our privacy policies. If the school wants to use personal data for reasons other than those given when this data was first obtained, the school will inform the individuals concerned before doing 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.

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 or parent/carer that puts the safety of our staff at risk We need to liaise with other agencies will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – 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 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.

Subject access requests and other rights of individuals

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 must be submitted in writing, either by letter or email 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.

Children and subject access requests

Personal data about a child belongs to that child. However, as all our children are aged 11 or below, apart from in exceptional circumstances, we would expect parents to act as owners of their children's data. Please see 9.1 above for subject access requests.

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 pupil 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 th e 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.

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.

Parental requests to see the educational record
Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

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 for photographs and videos to be taken of pupils 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 the parent/carer. Uses may include:

- Within school on notice boards, school posters, 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

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 child, beyond the first name, where necessary to ensure they cannot be identified.

12. 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

13. 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 or are password protected
- 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 it must be safeguarded, papers should be carried in locked bags or cases. The use by staff of removable media eg USB sticks is not permitted, unless password protected
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Staff, the chief executive officer or pupils 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 and Acceptable use agreements)
- 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)

14. 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.

15. CCTV

CCTV at LIFE SCHOOL is operated in accordance with GDPR. CCTV is configured to provide surveillance of:

- priority Security doors and gates that provide access to critical areas in which School functions are carried out;
- areas where business critical activity is carried out.

CCTV provides:

- Identification of persons entering and leaving the main entrances.
- Identification of staff entering and leaving the main entrances.
- Identification of persons moving between the boundary of public and private space.
- Observation of courier entrances/drop off points.
- Monitoring of external and internal parking.

Areas where CCTV surveillance systems are installed are clearly marked by relevant signs advising that such systems are in place. CCTV footage is stored and destroyed in accordance with the School's Records Retention Policy.

16. 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 Data Breach Procedure attached to this Policy.

When appropriate, we will report the data breach to the ICO within 72 hours. As example, 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 eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing personal data about pupils

17. Training

All staff and the chief executive officer 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.

18. References: References given by any member of School staff, whether for staff or students, may be given only with the consent of the Headteacher unless the reference is written by the Headteacher, in consultation with other staff where appropriate. Any reference will be fair, balanced and reasonable and will be provided in good faith. A request for a reference to be provided to an employer or institution overseas will be taken as the applicant's confirmation that the receiving country ensures an adequate level of protection for the rights and freedoms of Data Subjects. In exceptional circumstances the Headteacher may agree to provide a written testimonial. It should be noted that this does not constitute a reference or an open reference.

19. Links with other policies

This data protection policy is linked to our:

- Online Safety Policy
- Acceptable Use of ICT Agreements
- Child Protection and Safeguarding Policies
- Data Breach Procedure
- Freedom of information publication scheme
- Acceptable Usage policies
- Online Safety policy
- Record Management policy
- Privacy notices
- Internet, Network and Email Policy
- Use of CCTV Policy
- School Mobile Telephone Use 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 (who is INSERT ROLE) will alert the Chief executive officer

- 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 admin computer network, which is accessible by members of the admin team and the senior leadership team.
- 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 admin computer network, which is accessible by

members of the admin team and the senior leadership team.

- The DPO will 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

Non-anonymised pupil exam results or staff pay information being shared with the chief executive officer

- All paper documents recalled and shredded. If it is received by email, the chief executive officer must only access using their encrypted email and they will be asked to delete the info.
- The the chief executive officer confirm in writing that they have deleted the information.

A device containing non-encrypted sensitive personal data being stolen or hacked

- The incident will be reported to the police as soon as possible.

- If the device is a school registered device contact (the school IT supplier to wipe the device memory using appropriate software as soon as possible.
- If it is a personal device the member of staff must use their cloud supplier to wipe the device memory, they must confirm in writing that they have done this.
- Report to the DPO and assess what details could be accessible. The DPO will report to parents if suitable to the ICO

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

- The school will contact INSERT SCHOOL'S FINANCE SYSTEM immediately to find out details of the breach.
- Parents will be notified immediately and asked to change their passwords if they consider they may be at risk.