Data Protection Policy

Approved by: LIA Governing Board

Date of Ratification: October 2021

Frequency of Review: 3 Years

Next Review: October 202

CONTENTS

1. Introduction

The School is required to process personal data regarding staff, pupils and their parents and guardians, governors, trustees, volunteers, contractors and friends of the School relevant to its operation and shall take all reasonable steps to do so in accordance with this Policy.

Processing may include obtaining, recording, holding, handling, disclosing, transportation, destroying or otherwise using data. In this Policy any reference to pupils, parents, friends, volunteers, contractors, governors, trustees or staff includes current past or prospective individuals.

2. Legislation & 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 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.

3. Definitions

3.1. Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, roll number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual

3.2. Sensitive Personal Data

Any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings. The GDPR refers to sensitive personal data as "special categories of personal data".

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual The School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

- Explicit consent of the data subject must be obtained
- Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
- Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
- Data manifestly made public by the data subject
- Various public interest situations as outlined in the General Data Protection Regulations 2018

3.3. Data Subject

The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two pupils.

3.4. Data Controller

The School is the Data Controller and is responsible for determining the purposes of its use of data - what data it gathers and how this information is used. As the Data Controller the School is responsible for complying with the Act.

3.5. Data Protection Officer (DPO)

The School has appointed an external provider as its Data Protection Officer (Carole Connelly), responsible for day to day compliance with this Policy.

4. 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.

4.1 Governing Board

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.2. Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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

Our DPO is the School Business Manager contactable through the school office.

4.3. Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis

4.4. 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
- 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

5. Acquiring, Using and Disposal of Personal Data

The School shall only process personal data for specific and legitimate purposes. These are:

- providing pupils and staff with a safe and secure environment
- providing an education, training and pastoral care
- providing activities for pupils and parents - this includes school trips and activity clubs
- providing academic, examination and career references for pupils and staff
- protecting and promoting the interests and objectives of the School – this includes fundraising
- safeguarding and promoting the welfare of pupils
- monitoring pupils' and staff's email communications, internet and telephone use to ensure pupils and staff are following the School's IT Acceptable Use policy
- promoting the School to prospective pupils and their parents
- communicating with former pupils
- for personnel, administrative and management purposes. For example to pay staff and to monitor their performance
- fulfilling the School's contractual and other legal obligations

Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer's permission.

The School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

The School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or guardians living outside the EEA.

When the School acquires personal information that will be kept as personal data, the School shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

The School shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School's Document Retention Policy. Staff should not delete records containing personal data without authorisation.

The School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

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. 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

6. 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 – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and 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

7.Privacy Notices

Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement.

The privacy notice is to ensure that the School's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with, how long records will be retained for and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office

Copies of the School's privacy notice for pupils and parents can be obtained from the Data Protection Officer or accessed on the School's website.

8. Protecting Confidentiality

Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the data subject, unless they need to know it for a legitimate purpose.

Disclosing personal data outside of the School: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

Before sharing personal data outside the School, particularly in response to telephone requests for personal data staff should:

- make sure they are allowed to share it – that they have the necessary consent
- ensure adequate security. What is adequate will depend on the nature of the data.
- make sure that the sharing is covered in the privacy notice.

The School should be careful when using photographs, videos or other media as this is covered by the Act as well. Specific guidance on this is provided in the School's E Safety policy on the School's website.

Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches.

The School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening.

In particular:

- paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.
- the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.
- staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device. Further information is available from the Data Protection Officer.
- staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

9. Data Subject Rights

9.1. Subject Access Requests

Individuals are entitled to know whether the School is holding any personal data which relates to them, what that information is, the source of the information, how the School uses it and who it has been disclosed to. This is known as a Subject Access Request.

Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer.

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record. Any member of staff who receives a request for information covered by this policy from a pupil, parent or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timetable which the School must follow. Information must be provided to the requestor without delay and at the latest within one month of receipt.

Individuals have a right to ask the School not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

Individuals have a right to ask for incorrect personal data to be corrected or annotated.

Individuals have the right to object to any of their personal data being processed and to have this data erased.

Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.

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
- s 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.

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School Business Manager.

11. 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 their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, 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, to ensure they cannot be identified

12. 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.

13. 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.

14. Monitoring Arrangements

This policy will be reviewed by the headteacher every 3 years.

At every review, the policy will be approved by the full governing board.

15. Links with Other Polices

This policy is linked to the:

- Privacy Notices
- Acceptable Use Policy
- E-Safety Policy
- Staff Code of Conduct Policy
- Child Protection and Safeguarding Policy

Appendix 1 – Personal Data Breach Procedures

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 school's designated DPO Carole Connelly (carole@schooldposervice.com)

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.

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 will be stored securely electronically.

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)

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.

We will take the necessary actions 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.