St Edmund's Catholic Primary School

Data Protection Policy

Agreed By Governors: March 2023
Next Review Date: March 2026

1. Table Of Contents

2. Policy Statement

We need to collect and use personal information so that we can operate effectively as a school and fulfil our statutory duties. The information we collect and use includes information about pupils, parents, employees, governors, suppliers, visitors etc.

We are committed to protecting the privacy and security of this personal information at all times and supporting individuals in exercising their rights in relation to their own personal information.

This policy, along with accompanying procedures and associated policies, sets out our commitment and approach to safe data protection practice, as well as our support for individuals in exercising their rights. It applies to all personal data, regardless of whether it is in paper or electronic format.

It is reviewed annually and updated in line with any changes to data protection legislation.

3. Legislation

This policy meets the requirements of the UK General Data Protection Regulation (GDPR) and the provisions of the UK's Data Protection Act 2018.

Under the GDPR our school is classified as a Data Controller and we are registered with the UK's supervisory authority, the Information Commissioner's Office (ICO). Our registration is renewed annually.

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. This sits outside of the GDPR.

4. Contact

If you would like to discuss anything in this policy, please contact our Headteacher or Data Protection Officer (DPO) as follows:

Headteacher – Erika Kirwan head.3856@st-edmunds-rc.oxon.sch.uk
DPO - Nicola Cook, Schools DPO, nicola@schoolsdpo.com

5. Roles and Responsibilities

This policy applies to all staff employed by our school, as well as to external organisations or individuals working on our site.

Staff who do not comply with this policy may face disciplinary action, which could include dismissal. It is a criminal offence to access personal data held by the school for other than school business, or to procure the disclosure of personal data to a third party, or to sell such data.

The **Governing Board** has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The **Headteacher** has overall responsibility for ensuring the implementation of this policy. They will ensure that all staff are aware of their data protection obligations, and oversee

any queries related to the storing or processing of personal data.

The **Data Protection Officer** monitors compliance with data protection law, providing support and guidance as required.

5.1. All Staff

All Staff are responsible for ensuring that they process any personal data in accordance with this policy (a definition of processing can be found in Appendix 1). Staff must also inform the office of any changes to their personal data, such as a change of address.

Staff must contact the office whenever they have a query about data protection, including, but not limited to the following:

- any questions about the operation of this policy: including retaining personal data; keeping personal data secure; sharing personal data with third parties; or whether there is a lawful basis in place for a particular data processing operation
- any concerns that the policy is not being followed
- a new project under consideration that involves the processing of personal data
- received any requests from individuals for access to their personal information the school is processing.

6. Data Protection Principles

The UK GDPR sets out seven key principles which form the foundation of this data protection legislation:

- **Lawfulness, fairness and transparency** - Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- **Purpose limitation** - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- **Data minimisation** - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy** - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the

purposes for which they are processed, are erased or rectified without delay

- **Storage limitation** - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes. This is subject to implementation of the appropriate technical and organisational measures required by the GDPR, in order to safeguard the rights and freedoms of individuals

- **Integrity and confidentiality (security)** - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

- **Accountability** - the controller shall be responsible for, and able to demonstrate, accountability with the GDPR principles.

This **Data Protection Policy**, along with our privacy notices and additional policies and procedures referenced in section 25, sets out how our school aims to comply with these principles.

7. Lawfulness, fairness and transparency

7.1. Lawfulness

We will always ensure we have a valid lawful basis for our processing of personal data. There are six lawful bases we can rely on under the UK GDPR:

- **Contract** - the processing is necessary for a contract with an individual, or because they have asked for specific steps to be taken before entering into a contract.

- **Legal obligation** - the processing is necessary to comply with the law (not including contractual obligations).

- **Vital interest** - the processing is necessary to protect someone's life.

- **Public task** - the processing is necessary to perform a task in the public interest or for our official functions as a school, and the task or function has a clear basis in law.

- **Legitimate interests** - the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- **Consent** - the individual has given clear and informed consent for their personal data to be processed for a specific purpose. The individual can change their mind at any time and withdraw their consent. If this happens the processing will be stopped.

Some personal data is considered more sensitive under the GDPR, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sex life or sexual orientation.

For these **special categories** of personal data, we will also identify one of the special category conditions for processing set out in the GDPR:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law).

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1 part 1, paragraphs 1, 8 and 18. These relate to the processing of special category data for employment purposes, safeguarding and equality of opportunity/treatment.

Our Appropriate Policy Document provides more information about this processing. This is available in the policy folder of the Staff Shared Area and on the school website.

7.2. Criminal Convictions and Offences

The UK GDPR also gives extra protection to **criminal offence data**. As well as ensuring a valid lawful basis for the processing of criminal offence data under the GDPR, we will also identify an additional condition set out in Schedule 1 of the UK DPA 2018.

Under Article 6 of the GDPR, lawful bases we rely to process this data are:

- Performance of our **public task**
- Performance of a **contract**.

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1:

- Part 2, para 6(2)(a)
- Part 1, para 1.

These relate to the processing of criminal offence data for statutory and employment purposes respectively. See Part 3 of *Keeping Children Safe in Education* for more information.

Our Appropriate Policy Document provides more information about this processing. This is

available in the policy folder of the Staff Shared area and on the school website.

7.3. Fairness and transparency

Data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

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

This will normally be through our **privacy notices**:

Our **Privacy Notice for Pupils** sets out how we process pupil personal data to support teaching and learning, to provide pastoral care and to assess the performance of our services.

Our **Workforce Privacy Notice** sets out how we process the personal data of staff, agency staff and contractors to fulfil our obligations as an employer.

Our **Privacy Notice for Governors** sets how we process governors' personal data to support them in fulfilling their governance role.

All our Privacy Notices also include information on the rights of the individuals whose data we are processing and who to contact to discuss any aspect further.

8. Purpose limitation

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data (usually through our privacy notices).

If we want to use personal data for reasons other than those given when we first obtained it, we will identify and document a new lawful basis; although this may not be necessary if our new purpose is compatible with the original purpose. We will inform the individuals concerned before we do so, and seek consent where necessary.

9. Data minimisation

We will only collect the minimum amount of personal data necessary for our purposes. Staff will only process personal data where it is necessary to perform their roles.

10. Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject

informs us of a change of circumstances, their records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, we will immediately mark the record as potentially inaccurate, or "challenged".

11. Storage limitation

When our school no longer needs the personal data it is processing, it will be deleted or anonymised. This will be done in accordance with our data retention schedule, which can be found in the policy folder on the Staff Shared Area or on the school website.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use an outside company to convert paper records to electronic files and shred documents on site.

Where details of individuals are stored for long-term archive, historical or statistical reasons, this will be done within the requirements of the GDPR.

12. Security

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.

All members of staff are required to sign to confirm that they have read and understood this Data Protection Policy.

All members of staff are required to sign an acceptable user agreement which is renewed annually. The acceptable user agreement is linked to the school's Online Safety Policy and covers such aspects as:

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information being kept securely when not in use
- Papers containing personal information being kept secure and not being left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff ensuring that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended
- Staff adhering to school policies and procedures when taking data off site and when working remotely or at home
- Strong passwords being used to access school systems, online resources, laptops and other electronic devices. These must be at least 8 characters long containing letters and numbers; or preferably passphrases (e.g. 3 unconnected words).

- Encryption software being used to protect all portable devices and removable media
- Staff not storing personal information on their personal devices and being expected to follow the same security procedures as set out for any school owned equipment
- GDPR compliant cloud storage being used for all online data storage
- The use of USB devices not being allowed to store personal data.

13. Accountability

The school has put in place appropriate technical and organisational measures to meet the requirements of the accountability principle These include:

- The appointment of a data protection officer who reports directly to our highest management level
- Taking a 'data protection by design and default' approach to our activities
- Maintaining accurate documentation of our processing activities, such as the purposes of processing personal data, data sharing and retention. We also document the lawful bases and conditions we are relying on for our purposes, including how and when consent was obtained, as appropriate
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing (see section 6).

We regularly review our accountability measures and update or amend them when required.

14. Data Protection Impact Assessments

The GDPR requires us to carry out Data Protection Impact Assessments (DPIAs) for any type of processing that is likely to result in a high risk to individuals' interests; for example, when introducing new technologies, or using biometric data for identification purposes.

To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk can result from either a high probability of some harm, or a lower possibility of serious harm.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

As part of our data protection by design and default approach we will carry out a DPIA for any other major project which requires the processing of personal data.

We follow the ICO's guidelines and our DPIAs:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks.

15. 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 who 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 United Kingdom, we will do so in accordance with the international transfer rules in the GDPR .

Where we share personal data on an ad hoc or 'one off' basis, we will record the details including our purpose and lawful basis for doing so

16. Subject Access Requests

Under the GDPR, anyone whose personal data we are processing, e.g staff, pupils and parents\carers etc, has a right to make a 'subject access request' to gain access to information our 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 can be made by contacting any member of staff, but it is helpful if they are made to the School Office or the DPO. They can be made in person, verbally, in writing, and by email. The following information will be required:

- Name of individual
- Relationship of the requester to the individual, if appropriate
- Correspondence address
- Contact number and email address
- Details about the information requested

Completion of a subject access request form can be useful, but this cannot be insisted upon.

If a member of staff receives a subject access request they must immediately forward it to the School Office.

Members of staff can find further information on their role in handling subject access requests in our Guidance for Staff.

16.1. Children and Subject Access Requests

A child's personal data always belongs to them rather than the child's parents or carers. For a parent or carer to make a subject access request, with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

The UK's Information Commissioner's Office generally regards children aged 12 and above to be mature enough to understand their rights and the implications of a subject access request. However, we will always consider this on a case by case basis.

16.2. Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification, if necessary
- 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 reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Any references that have been provided or received in confidence.

If the request is considered 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 considered 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.

17. Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it (see section 6), 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 United Kingdom
- 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)

If staff receive such a request, they must immediately forward it to the school office.

18. Parental Requests to access their Child's Educational Record

In maintained schools, parents have a separate right to access their child's educational record under the Education (Pupil Information, England) Regulations 2005. The request must be made in writing and the information will be provided within 15 school days of receipt of the request.

19. Photos and Videos

As part of our educational activities, we may take photographs and record images of individuals. We will always clearly explain to pupils and/or parents (as appropriate) how the photograph or video will be used.

We will obtain consent for photographs and videos to be taken of pupils for marketing and promotional materials.

Uses may include:

- 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 page.

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 individual, except first names if parents agree, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of

photographs and videos.

20. Personal Data Breaches

The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

When a personal data breach has occurred we will assess the likelihood and severity of the resulting risk to the rights and freedoms of the individuals involved. If it's likely that there will be a risk, then we are required by law to notify the ICO.

20.1. Data Breach Register

We record all breaches of personal data, regardless of whether they are reported to the ICO. Our data breach register includes the details of the breach, its effects and any remedial action taken. Remedial action may include a review of relevant systems or policies and procedures; additional training for staff; or other corrective steps, as appropriate.

21. Data Breach Response Plan

Each breach will be considered on a case by case basis and our Data Breach Response Plan, included as an appendix to this policy, sets out in more detail the procedures we will follow.

If any member of staff believes a breach of personal data has occurred, or might have occurred, they are required to let the headteacher know immediately.

22. Training

Our staff are provided with data protection training as part of their induction process and this is refreshed at least annually. We take a blended approach, so training may be formal CPD - face to face or online delivery; through INSET days, staff meeting updates and discussion, 1:1 reviews, newsletters etc.

Uptake of training is monitored and procedures are in place to ensure that all staff complete the required training.

23. Concerns and Complaints

We will always endeavour to resolve any concerns an individual may have about our processing of their personal data informally. However, if this is not possible, the individual will be advised to use our school's complaints procedure. If, after this, the individual remains concerned, they will be advised how they can raise those concerns with the ICO.

24. Monitoring Arrangements

The Governing Board is responsible for monitoring and reviewing this policy. It will be reviewed on an annual basis.

25. Links with Other Policies and Procedures

This Data Protection Policy is linked to:

- Privacy Notice for Pupils
- Workforce Privacy Notice
- Privacy Notice for Governors
- Use of Email Policy/Acceptable User Agreements
- Record Retention Schedule
- Guidance for Staff on Subject Access Requests
- Data Breach Response Plan
- Appropriate Policy Document
- ICT Security/E-safety Policy
- Child Protection Policy/Safeguarding Policy
- Freedom of Information Publication Scheme.

26. Appendix One - Definitions

Term	Definition
Personal data	Data from which a person can be identified (i.e. distinguished from other individuals); such as: • Name (including initials) • Identification number • Location data • email address, telephone number, car registration number • Online identifier, such as a username, IP addresses, cookie identifiers • photographs, video recordings This includes data that, when combined with other readily available information, leads to a person being identified.
Special category persona data	Personal data which is more sensitive and is therefore afforded more protection under the GDPR. Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or philosophical beliefs • Where a person is a member of a trade union • genetic data • biometric data (when used for identification purposes) • Physical and mental health • Sexual orientation and sex life Data relating to criminal convictions is afforded similar special protection.
Processing	Any operation carried out on personal data, such as collecting, recording, storing, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The living individual whose personal data is held or processed.

Data controller	A person, or organisation, that determines the purpose for which, and the way, personal data is processed.
Data processor	A person, or other body, other than an employee of the data controller, who processes the 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. Breaches can be the result of accidental or deliberate causes.

27. Appendix Two Data Breach Response Plan

1. Introduction

This data breach response plan is an appendix to our school's Data Protection Policy which it should be read in conjunction with. If you have any queries, please contact Erika Kirwan, our Data Protection Lead in the first instance.

The General Data Protection Regulation (GDPR) defines a personal data breach as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

A breach of personal data is a type of security incident and falls into one of three categories:

1. "Confidentiality breach" - an unauthorised or accidental disclosure of, or access to, personal data
2. "Integrity breach" - an unauthorised or accidental alteration of personal data
3. "Availability breach" - an accidental or unauthorised loss of access to, or destruction of personal data.

A breach may concern the confidentiality, integrity and availability of personal data at the same time, or any combination. It can be the result of both accidental and deliberate causes.

Some examples of personal data breaches include:

1. access by an unauthorised third party (including the malicious acts of hackers

and scammers)
2. deliberate or accidental action (or inaction) by a controller or processor
3. sending personal data to an incorrect recipient
4. computing/mobile devices containing personal data being lost or stolen
5. alteration of personal data without permission
6. loss of availability of personal data, e.g. when it has been encrypted by ransomware, or accidentally lost or destroyed (including natural disasters such as fire and flood).

Under the GDPR any breach of personal data requires mandatory notification to our supervisory authority, the Information Commissioner's Office (ICO); unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

2. When a Breach of Personal Data Occurs

As soon as we are aware* that a breach of personal data has occurred, we will immediately seek to contain the incident and also assess the risk to the rights and freedoms of the individual(s) involved.

*Awareness of a breach occurs when we have a reasonable degree of certainty that a breach has occurred.

The GDPR requires us to use our resources to ensure we are 'aware' of a data breach in a timely manner. In some cases it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised.

A data incident/breach may occur during school holidays when the school is closed or we have a reduced number of staff available. We will ensure that all members of staff have the contact details of the Data Protection Lead and DPO so that any incident/breach can still be dealt with appropriately. These contact details are also included in our Data Protection Policy and Privacy Notices, which are available on our website.

3. Assessment of Risk

The risk from a breach is assessed on a case by case basis and both the severity of the potential impact on the rights and freedoms of the individuals and the likelihood will be considered.

When assessing the risk to individuals as a result of a personal data breach we will consider:

1. The type of breach
2. The nature, sensitivity and volume of the personal data
3. How easy it is to identify individuals
4. The severity of consequences for individuals
5. Special characteristics of the individual, e.g. if they are children
6. Any special characteristics of our school
7. The number of affected individuals.

A breach is likely to result in a risk to the rights and freedoms of individuals if it could result in physical, material or non-material (e.g.emotional) damage. In particular:

1. Loss of control over personal data
2. Limitation or deprivation of individuals' rights
3. Discrimination
4. Identity theft or fraud
5. Financial loss
6. Damage to reputation
7. Unauthorised reversal of pseudonymisation
8. Loss of confidentiality of personal data protected by professional secrecy
9. Any other significant economic or social disadvantage.

Where special category data* is involved, the GDPR states that such damage should be considered to be likely to occur.

*Special category data is data that is considered more sensitive and requires greater protection: racial or ethnic origin, political opinion, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or sex life, or biometric data used for identification purposes. Data relating to criminal convictions is afforded similar special protection.

4. Notification to the ICO

As a result of this assessment, if we believe that there is a risk to the rights and freedoms of the individual(s), we will notify the Information Commissioner's Office, as required under the GDPR. If we are in any doubt, we will always err on the side of caution and notify the ICO.

Where we assess a breach is reportable to the ICO, we must make this report without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.

As a minimum, we must include in our notification:

1. description of the nature of the personal data breach including, where possible:
    - categories and approximate number of individuals concerned
    - categories and approximate number of personal data records concerned
2. name and contact details of the DPO
3. description of the likely consequences of the personal data breach
4. description of the measures that have been, or will be taken, to deal with the breach and individual(s) concerned.

The GDPR makes no allowance mitigate any possible adverse effects on the in the statutory reporting timescale of 72 hours for breaches that occur during school holidays. Therefore, it is important that staff contact the school Data Protection Lead and the DPO as soon as possible.

5. Communication to affected individuals

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify affected individuals as soon as possible. We will provide:

1. A description of the nature of the breach
2. The name and contact details of the DPO and/or Data Protection Lead
3. A description of the likely consequences of the breach
4. A description of the measures taken or proposed to be taken, by the school to address the breach and mitigate any possible adverse effects.

We will also consider what specific advice we can provide to individuals to help them protect themselves, such as resetting passwords where access credentials have been compromised.

6. Roles and Responsibilities

All Staff - if any member of staff believes a breach of personal data has occurred, or might have occurred, they must immediately notify the Data Protection Lead Erika Kirwan who will liaise with the Data Protection Officer:

Nicola Cook, SchoolsDPO Ltd:
01296 658502, nicola@schoolsdpo.com.

If members of staff receive personal data sent in error they must alert the sender and the **Data Protection Lead** as soon as they become aware of the error.

The **Data Protection Lead**, with the support of colleagues, will investigate the report, and determine whether a breach has occurred. To decide, they 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 **Data Protection Lead** will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

In discussion with the **Data Protection Lead**, the **DPO** will assess the potential consequences of the breach and advise whether the breach needs to be reported to the ICO.

If the breach is likely to be a risk to the people's rights and freedoms, the **DPO** will notify the ICO.

Where a breach is likely to result in a high risk to people's rights and freedoms, the **Data**

Protection Lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will include:

- 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.

2. The **Data Protection Lead** will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
3. The **Data Protection Lead** will document each breach, irrespective of whether it is reported to the ICO and ensure a record is kept in the Data Breach Register.

7. Actions to minimise the impact of data breaches

The type of action we might take will depend on the nature of the breach, but could include (this list is not exhaustive):

1. Attempting to recover lost equipment
2. Remotely wiping electronic devices
3. Using of back-ups to restore lost/damaged/stolen data
4. Changing entry codes or IT system passwords
5. Attempting to recall emails containing personal information that are sent to unauthorised individuals
6. Requesting personal data received in error is deleted and written confirmation is provided that the information has been deleted, and not shared, published, saved or replicated in any way
7. Carrying out internet searches to check information hasn't been made public. If it has, asking the publisher/website owner/administrator to remove and destroy the information
8. Briefing staff in case of phishing enquiries for further information on affected individuals
9. Notifying the Local Authority.

We will review the effectiveness of any actions taken and amend them as necessary after any data breach. This may include establishing more robust policies and procedures or providing further training for staff.

8. Accountability and Record Keeping

We record all breaches of personal data regardless of whether they are reported to the ICO. This helps us demonstrate our compliance with the GDPR under its principle of accountability. It also ensures we have records should the ICO wish to see them.

Our data breach register includes:

1. Summary of the facts:
    - including the types and amount of personal data involved
    - details of the cause of the breach and impact on the individuals whose data is involved
2. Actions taken to contain the breach as well as mitigate its possible adverse effects
3. Any actions taken to prevent future breaches.