DATA PROTECTION POLICY

Potten End Church of England Primary School

Policy Review

This policy was agreed by the Governing Board on……12/02/2026……..

It is due for review on…February 2027……

Signature ……. Date ……

Head Teacher

Signature ……. Date ……

Chair of Governors

Rooted in faith, we nurture, grow and flourish

1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that Potten End CE Primary (the "School") and its governors and employees are informed about, and comply with their obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and any other relevant data protection legislation.

1.2 The School is a VC (Voluntary Controlled) school and is the Data Controller for all the Personal Data processed by the School. For the avoidance of doubt, any reference to School refers to the "corporate body" or entity of the school which is represented by it's Headteacher (or other nominated/approved individuals or groups) and not the physical buildings or its fabric.

1.3 Everyone has rights about how their personal information is handled. During our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

1.4 The type of information that we may be required to handle includes details of job applicants, current, past and prospective employees, pupils, parents / carers and other members of pupils' families, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in UK GDPR and other legislation. The UK GDPR imposes restrictions on how we may use that information.

1.5 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. A breach of UK GDPR may expose the School to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the School's employees. At the very least, a breach of UK GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

2. Status of the policy

2.1 This policy has been approved by the Governing Body of the School. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3.0 Roles and responsibilities

3.1 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.

3.2 Governing Body

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

3.3 Data Protection Officer

The Data Protection Officer (DPO) plays a major role in embedding essential aspects of UK GDPR into the School's culture, from ensuring the data protection principles are respected, to preserving individuals rights, recording data processing activities and ensuring the security of processing. The 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.

They will provide a regular report of their activities directly to the Governing Board at each FGB, maintain and monitor activities and, where relevant, report to the board their advice and recommendations on school data protection issues.

If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO. The DPO is also the first point of contact for the Information Commissioner's Office (ICO). The post of DPO is held by Emma Harris (Governor) and can be contacted either via the school office or email DPO@pottenend.herts.sch.uk

3.4 Headteacher

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

3.5 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 UK, including to countries outside the UK that are not covered by an adequacy regulation (international transfers of personal data)
- 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

4. Definition of terms

4.1 **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

4.2 **Consent** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

4.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

4.4 **Data Subjects** (individuals) for the purpose of this policy include all living individuals about whom we hold Personal Data. Data Subject (individuals) need not be a UK national or resident. All individuals have legal rights in relation to their Personal Data;

4.5 **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;

4.6 **Data Users** include employees, volunteers, governors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;

4.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

4.8 **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

4.9 **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

4.10 **Personal Data Breach** means 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;

4.11 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UK GDPR;

4.12 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.13 **School** means the school as an entity represented by the Headteacher or other approved/nominated representatives and not the physical buildings themselves.

4.14 **Special category personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

4.15 Data protection principles

UK 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

5. Collecting personal data

5.1 This policy sets out how the school aims to comply with these principles.

5.2 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 authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

5.3 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in UK GDPR and Data Protection Act 2018. For most of our core teaching, safeguarding and administrative functions we will usually rely on the public task or legal obligation lawful bases, not consent.

5.4 Where we rely on consent, we will make sure that consent is clear, specific, freely given and can be withdrawn at any time.

5.5 When we use online services that are likely to be accessed by children, we will follow the ICO's Children's Code (age-appropriate design code) and make sure any privacy information is easy for children to understand.

5.6 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. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do 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.

5.7 Criminal convictions and offences

There are separate safeguards in UK GDPR for Personal Data relating to criminal convictions and offences.

It is likely that the School will process data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or parents. This information is not routinely collected and is only likely to be processed by the School in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

6. Sharing personal data and information

6.1 We will not normally share personal data or information 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 Support contractor. 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 and information 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.

Where we need to share personal data to keep a child or vulnerable person safe, we will do so in line with our safeguarding duties, Keeping Children Safe in Education and current DfE and ICO guidance on data sharing for safeguarding

We may also share personal data and information with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

6.2 Governors

Governors should be trained on the School's data protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

- Ensuring that Personal Data which comes into their possession as a result of their School duties is kept secure from third parties, including family members and friends.

- Using a School email account for any School-related communications.

- Ensuring that any School-related communications or information stored or saved on an electronic device or computer is password protected.

- Taking appropriate measures to keep Personal Data secure, including ensuring that hard copy documents are securely locked away so that they cannot be accessed by third parties

Governors will be asked to read and sign an Acceptable Use Agreement.

7. Processing in line with Data Subjects' rights

Individuals have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside the UK, including to countries outside the UK that are not covered by an adequacy regulation (international transfers of personal data);
- prevent Processing that is likely to cause damage or distress to the individual or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority (the ICO);
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff will not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

8. Subject access requests

8.1 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.

8.2 Individuals can make a subject access request verbally or in writing (for example by letter, email or in person). To help us deal with requests quickly and accurately, we may ask the requester to put their request in writing or to clarify what information they need. Requests should be sent or directed to the DPO. To help us identify the information requested, they should, where possible, include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

8.3 If staff receive a subject access request, whether verbally or in writing, they must immediately forward it to the DPO.

8.4 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the individual does not specifically use this phrase in their request or refer to UK GDPR. Requests for information will be dealt with without undue delay and within **one month** from the date we receive the request. In some cases (for example if the request is complex or there are many requests) we may extend this by up to a further two months. If we need to do this, we will tell the requester within the first month and explain why.

8.5 We will make sure that subject access requests can still be received and managed during school holiday periods. This may include checking the DPO email account regularly and arranging access to our systems if needed.

8.6 The School may ask the individual for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

8.7 Subject access rights belong to the pupil. A parent can make a subject access request for information about their child only where:

- the child is not able to make their own request (for example because of age or maturity), or
- the child has clearly authorised the parent to act for them.

When we receive a request from a parent, we will consider the child's age, maturity and best interests when deciding whether to provide the information and whether to consult the child.

8.8 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made in the School's Subject Access database, showing the date of receipt, the Individual's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information. Should more information be required to establish either the identity of the Individual (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

8.9 Where requests are "manifestly unfounded or excessive", because they are repetitive, the School can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

8.10 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.

Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from

disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly.

8.11 In the context of a School a subject access request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee.

8.12 When responding to a subject access request, we will carry out searches that are reasonable and proportionate. We are not required to provide copies of documents that do not contain the requester's personal data or information the requester already has access to. If we need the requester to clarify their request, we may pause ('stop the clock on') the time limit while we wait for this clarification, in line with current law and ICO guidance.

8.13 Parents' right to see the educational record

This policy explains how we deal with subject access requests (SARs) under the UK GDPR.

In addition, because we are a maintained school, parents have a separate right under education law to ask for a copy of their child's educational record.

A parent's right to the educational record only covers information that is part of that record, and we must respond within 15 school days of receiving a written request.

A SAR gives the pupil a broader right to access their personal data, and we must respond within one month (with limited scope to extend this where the law allows).

When a parent asks for information, we will decide whether the request is for the educational record, a SAR, or both, and we will explain which rules and time limits apply.

Further details about parents' rights to the educational record are set out in the Education (Pupil Information) (England) Regulations 2005

9.14 Processing in line with Data Subjects' rights

If someone is unhappy with how we have used their personal data, we encourage them to raise the issue with the DPO first so we can try to resolve it. We will acknowledge data protection complaints within 30 days and will respond without undue delay. Individuals also have the right to complain to the Information Commissioner's Office (ICO) if they are not satisfied with our response.

9.15 Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the School, whilst also applying common sense to the circumstances. They will be entitled to:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

9.16Authorised disclosures

The School will only disclose data about individuals if one of the lawful bases apply.

Only authorised and trained staff are allowed to make external disclosures of Personal Data. The School will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Local Authorities
- the Department for Education
- the Diocese of St. Albans
- the Disclosure and Barring Service
- the Teaching Regulation Agency
- the Teachers' Pension Service
- the Local Government Pension Scheme which is administered by
- Our external IT Provider
- HMRC
- the Police or other law enforcement agencies
- insurance providers
- occupational health advisors

- Ofsted
- NHS health professionals including educational psychologists and school nurses;
- Education Welfare Officers;
- Courts, if ordered to do so;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;

Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches.

Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

9.17 All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

9.18 The UK GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is Processed ("GDPR clauses"). A summary of UK GDPR requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the School to ensure that UK GDPR clauses have been added to the contract with the Data Processor. Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

In some cases Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with UK GDPR, including responsibility for any Personal Data Breaches, onto the School. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

10 Reporting a Personal Data Breach

10.1 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.**

10.2 When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

10.3 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the data breach is unlikely to result in a risk to the individuals.

10.4 If the breach is likely to result in high risk to affected Individuals, UK GDPR, requires organisations to inform them without undue delay.

10.5 It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

10.6 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Individuals or any applicable regulator where we are legally required to do so.

10.7 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, the DPO must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

11 Record keeping

The UK GDPR requires us to keep full and accurate records of all our Data Processing activities.

We must keep and maintain accurate records reflecting our Processing including records of Individuals' Consents and procedures for obtaining Consents.

These records should include, at a minimum;

- the name and contact details of the Data Controller and the DPO,
- clear descriptions of the Personal Data types,
- Individual types,
- Processing activities,

- Processing purposes,
- third-party recipients of the Personal Data,
- Personal Data storage locations,
- Personal Data transfers,
- the Personal Data's retention period and
- a description of the security measures in place.

In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

12 Training and audit

We are required to ensure all School personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

Members of staff must attend all mandatory data privacy related training.

13 Policy Review

13.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

13.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

14 Enquiries

Further information about the School's Data Protection Policy is available from theDPO.

General information about the UK GDPR can be obtained from the Information Commissioner's Office: www.ico.org.uk

Document Control

Date modified	Description of modification	Modified by
19/05/2024	Clarification that sharing of Personal Data applies to all information, not just electronically held records.	R.Dale & E.Harris
11/02/2026	Refining wording to align with current regulations (UK GDPR) and Data Use and Access (2025) Act. Update on definition of consent, children's rights and access to their personal information in line with ICO recent revisions. Amend to wording to align with guidance from ICO and DfE, update to ICO web address. Amend to clarify SAR process. Additional section separating Parental rights to access child's educational record (in line with Education (Pupil Information) (England) Regulations 2005. Minor wording changes to improve readability	E Harris

Appendix 1 – Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the Headteacher and the Chair of Governors.
The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (Actions relevant to specific data types are set out at the end of this procedure).
The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- 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 GovernorHub file system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored securely on the school's GovernorHub.

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. The DPO will also provide an update to all Governors by email or at the next available FGB, depending on the severity.

Appendix 2 - GDPR Clauses

UK GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in UK GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3) (a))

2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3) (b))

3. The Processor must keep Personal Data secure. (Art. 28(3) (c) Art. 32)

4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3) (d))

5. The Processor must ensure it flows down UK GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))

6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3) (e))

7. The Processor must assist the Data Controller with their security and data breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3) (f)) (Art. 33(2))

8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3) (f))

9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3) (g))

10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3) (h))

11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3))