GDPR policy

Policy version:	1.5
Policy Owner:	Principal – Phoenix Bay
Applies to:	Phoenix Bay School
Linked policies:	• E-safety policy • Safeguarding and child protection policy • Lone working policy
Review frequency:	Annually
AB Adoption Date:	September 2021
Date of recent review:	September 2026
New review date:	September 2027
Approved by:	Ross Banks – Principal  Jill Bainton – Advisory board

Version Control since September 2021

Version	Date of Change/Adopted	Reviewed by	Reason for change
1.0	September 2021	R Banks	New document
1.1	October 2022	R Banks/Jill Bainton	Revised
1.2	October 2023	R Banks/Jill Bainton	No changes made
1.3	October 2024	R Banks/Jill Bainton	No changes made
1.4	September 2025	R Banks/Jill Bainton	No changes made
1.5	September 2026	R Banks	Updated data protection legislation and strengthened key procedures.

Policy contents:

1	Aims
2	Legislation and Guidance
3	Definitions
4	The Data Controller
5	Roles and Responsibilities
6	Data Protection Principals
7	Collecting Personal data
8	Sharing personal data
9	Subject access requests and other rights of individuals
10	Parental requests to see the education record
11	Photos and videos
12	Data protection by design and default
13	Data security and storage of records
14	Disposal of records
15	Personal data breaches
16	Training
17	Appendix 1: Personal data breach procedure

1. Aims

Phoenix Bay School aims to ensure that all personal data collected about staff, students, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025

It is based on guidance published by the Information Commissioner's Office (ICO) on data protection and the UK GDPR.

The school will keep this policy under review to ensure it reflects changes to data protection legislation, ICO guidance and the school's data processing activities.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ◊ Name (including initials) ◊ Identification number ◊ Location data ◊ Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents/carers, students, staff, governors, visitors and others, and therefore is a data controller.

5. 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.

5.1 Directors

The Directors have overall responsibility for ensuring that Phoenix Bay complies with all relevant data protection obligations.

5.2 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.

They will provide an annual report of their activities directly to the Principal and, where appropriate, provide advice and recommendations on school data protection matters.

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

Our DPO is Jacqui Sloane and is contactable via 01803 220750,
email j.sloane@phoenixbay.co.uk.

5.3 Principal

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

5.4 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
    - If there has been a data breach or suspected 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

6. Data protection principles

The 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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have a lawful basis to do so under data protection law.

These lawful bases include:

- 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 protect the **vital interests** of the individual or another person, for example to protect someone's life
- The data needs to be processed for the **legitimate interests** of the school or a third party, provided that the individual's rights and freedoms do not override those interests
- The individual has freely given clear **consent** to the processing of their personal data

Where we process personal data for another lawful basis permitted under the UK GDPR, we will ensure that the relevant lawful basis is identified and documented.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law. These may include:

- The individual has given **explicit consent**
- The processing is necessary for the purposes of carrying out obligations or exercising specific rights in relation to employment, social security or social protection law

- The processing is necessary to protect the **vital interests** of the individual or another person where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The processing is necessary for the establishment, exercise or defence of **legal claims**
- The processing is necessary for reasons of **substantial public interest** as defined in legislation
- The processing is necessary for **health or social care purposes**, subject to the requirements of data protection law
- The processing is necessary for **public health reasons**, subject to the requirements of data protection law
- The processing is necessary for **archiving purposes, scientific or historical research purposes, or statistical purposes**, where the relevant legal conditions are met

For criminal offence data, we will identify both a lawful basis under Article 6 UK GDPR and an appropriate condition under Article 10 UK GDPR and the Data Protection Act 2018.

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We will only share personal data where we have a lawful basis to do so under UK GDPR. In many cases this will not require consent.

These include, but are not limited to, situations where:

- There is an issue with a student 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 students – for example, IT companies. When doing this, we will:
  - ◊ Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
  - ◊ Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 students or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

A subject access request can be made verbally or in writing, including by email or other electronic communication. Individuals do not have to use specific wording or refer to data protection legislation for a request to be valid.

A subject access request may include requests for:

- 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 is not possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data and, where applicable, information about the significance and consequences of this processing
- The safeguards provided if personal data is transferred internationally

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

9.2 Children and subject access requests

The right of access belongs to the child.

Where a parent, person with parental responsibility or another individual makes a subject access request on behalf of a child, the school will consider whether the child is competent to exercise their right of access and whether it is appropriate for the request to be made on their behalf.

The school will assess the child's competence on a **case-by-case basis**, taking into account their age, maturity and level of understanding of the nature and implications of the request.

There is no fixed age at which a child in England is automatically considered competent to make a subject access request.

Where appropriate, the school may seek the child's views before deciding whether information should be disclosed.

The school will also consider whether any exemptions or restrictions apply before providing information relating to a child.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide information reasonably necessary to confirm their identity where this is required
- Will respond without undue delay and normally within **one month** of receiving the request, or from the date on which any information reasonably required to confirm the individual's identity is received
- Will provide the information free of charge in most circumstances
- May extend the response period by up to a further **two months** where necessary because the request is complex or the individual has made a number of requests. Where this applies, we will inform the individual within the first month and explain why the extension is necessary
- Will carry out a reasonable and proportionate search for relevant personal information
- Will provide the information in a clear and accessible form
- Will take reasonable steps to ensure that information is provided securely

We may refuse to comply with a request, or charge a reasonable fee, where the request is **manifestly unfounded or excessive**, in accordance with data protection law.

When we refuse a request, we will tell the individual why and inform them of their right to complain to the ICO or seek to enforce their right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request, individuals also have the right, where applicable, to:

- Withdraw their consent to processing at any time where consent is the lawful basis
- Ask us to rectify inaccurate or incomplete personal data
- Ask us to erase their personal data in certain circumstances
- Ask us to restrict processing in certain circumstances
- Object to processing in certain circumstances
- Challenge decisions based solely on automated decision-making where applicable
- Make a complaint to the ICO
- Request data portability in certain circumstances

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Phoenix Bay School is an independent school and is not obliged to provide access to a pupil's educational record under the Education (Pupil Information) (England) Regulations 2005.

However, individuals may have rights of access to personal information held by the school under UK data protection legislation, including the right to make a subject access request.

Where a parent, person with parental responsibility or student requests information held by the school, the school will consider the request under the appropriate legal framework and will provide access where required by law.

The school will also consider any applicable exemptions, restrictions, safeguarding considerations and the rights of other individuals before information is disclosed.

11. Photographs and videos

As part of our school activities, we may take photographs and record images or videos of individuals within our school.

The school will identify an appropriate lawful basis for taking and using photographs and videos. Where **consent** is being relied upon as the lawful basis, consent will be obtained from parents/carers, or from the individual where appropriate.

Where consent is required, the school will clearly explain how the photograph or video will be used and who it may be shared with.

Photographs and videos may be used for purposes including:

- Within school on notice boards and in school magazines, brochures, newsletters and other school communications
- For educational or school activity purposes
- Outside of school by external agencies, such as the school photographer or newspapers, where appropriate
- Online on the school website or official social media pages, where appropriate

Where consent is the lawful basis, consent can be refused or withdrawn at any time. Where consent is withdrawn, the school will stop using the photograph or video for the relevant consent-based purpose and, where reasonably possible, remove it from future use.

The school will take reasonable steps to ensure that photographs and videos are used appropriately and securely and are not accompanied by unnecessary personal information that could identify a child.

Parents/carers taking photographs or videos at school events for their own personal use are generally not subject to UK data protection legislation in respect of that personal use. However, the school may ask parents/carers not to share photographs or videos of other students publicly, particularly on social media, for safeguarding and privacy reasons.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
  - ◊ For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

◊ For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices containing personal data are kept secure and locked away when not in use
- Papers containing confidential personal data must not be left on office or classroom desks, staffroom tables, or anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the school's procedures for signing it in and out and keeping it secure
- Staff must use strong passwords or passphrases and follow the school's requirements for account security and multi-factor authentication where provided
- Encryption or equivalent security measures will be used to protect portable devices and removable media containing personal data where appropriate
- Staff, students or governors who store personal information on personal devices must follow the school's security procedures and any requirements set out in the Online Safety Policy and Code of Conduct
- Where we need to share personal data with a third party, we will carry out appropriate due diligence and take reasonable steps to ensure that it is stored securely and adequately protected
- Access to personal data will be restricted to individuals who need it for legitimate school purposes
- Staff must not use personal email accounts or unauthorised cloud storage to store or transfer school personal data
- Personal data must only be accessed, downloaded, copied or shared where this is necessary for legitimate school purposes

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The school will make all reasonable endeavours to prevent personal data breaches and to minimise the impact of any breach that occurs.

A personal data breach includes the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In the event of a suspected or actual personal data breach, staff must report it to the DPO **immediately**, even if they are unsure whether a breach has occurred.

The school will assess each suspected breach to determine:

- What personal data is involved
- How many individuals may be affected
- The potential consequences for those individuals
- What steps can be taken to contain and minimise the breach
- Whether the breach is required to be reported to the ICO
- Whether the affected individuals need to be informed

Where a breach is reportable to the ICO, the school will notify the ICO **without undue delay and, where feasible, within 72 hours of becoming aware of the breach**.

Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, the school will notify those individuals without undue delay, unless an exception applies under data protection law.

All personal data breaches will be documented, including breaches that are not reported to the ICO. The record will include the facts surrounding the breach, its effects, the action taken to contain it and any measures introduced to prevent a recurrence.

The DPO and Principal will review significant breaches and identify any lessons, changes to procedures or additional staff training required.

16. Training

All staff 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.

17. Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by emailing j.sloane@phoenixbay.co.uk

- 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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - ◊ A description of the nature of the personal data breach including, where possible:
        - o The categories and approximate number of individuals concerned
        - o 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - ◊ A description, in clear and plain language, of the nature of the personal data breach
  - ◊ 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - ◊ Facts and cause
  - ◊ Effects
  - ◊ Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system. The DPO and Principal 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 and Principal will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.