Reviewed: October 2024
Next Review Date: October 2025

Signed by:

Claire Jones	Headteacher	Date: October 2024
Andy Oddy	Chair of Governors	Date: October 2024

Euxton Primrose Hill School Data Protection Policy

Table of Contents

Data Protection Policy

The following policy relates to all Euxton Primrose Hill Primary School employees (including voluntary, temporary, contract and seconded employees), who capture, create, store, use, share and dispose of information on behalf of Euxton Primrose Hill Primary School.

These persons shall be referred to as 'Users' throughout the rest of this policy. Euxton Primrose Hill Primary School shall be referred to as 'the school' or 'we' throughout the rest of this policy.

The following policy relates to all electronic and paper based information.

Statement of Commitment

In order to undertake our statutory obligations effectively, deliver services and meet customer requirements, the school needs to collect, use and retain information, much of which is personal, sensitive or confidential.

Such information may be about:

- Pupils
- Parents and Carers
- Governors
- Employees or their families
- Members of the public
- Business partners • Local authorities or public bodies.

We regard the lawful and correct treatment of personal data by the school as very important to maintain the confidence of our stakeholders and to operate successfully.

To this end, the school will ensure compliance, in all its functions, with the Data Protection Act (DPA) 2018 and the UK General Data Protection Regulation (UK GDPR), and with other relevant legislation.

Roles and responsibilities

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

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

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

They will provide an annual report of their activities directly to the Governors and senior leaders and, where relevant, report to the board their advice and recommendations on trust data protection issues.

Data Protection Principles

The Principles of DPA and UK GDPR state that personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals; the lawful basis can be:

   - Consent of a data subject
   - Processing is necessary for the performance of a contract with the data subject
   - Processing is necessary for compliance with a legal obligation (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014)
   - Processing is necessary to protect the vital interests of the data subject or another person (e.g. life or death)
   - Processing is necessary for the performance of a task carried out in the public interest

   The lawful basis for sensitive personal data (racial, political, religious, trade union, genetic, health, sex life, criminal convictions or offences) is:

   - Explicit consent of the data subject
   - Processing is necessary for carrying out obligations under employment, social security or social protection law
   - Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
   - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent
   - Processing relates to personal data manifestly made public by the data subject
   - Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
   - Processing is necessary for reasons of substantial public interest
   - Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services
   - Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
   - Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article
     - 89(1)

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. Accurate and, where necessary, kept up to date

5. 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

6. Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Compliance with the Data Protection Principles and Data Protection Legislation

In order to comply with these principles and meet all data protection obligations as stipulated in data protection legislation, the school will:

- Raise awareness of data protection across the school.
- Offer data protection training to all employees and governors.
- Create a data protection policy for the school that is updated annually.
- Complete a personal data processing audit, which lists the following:
    - Name of the personal data set.
    - Purpose for processing this personal data set.
    - Who the data set is shared with.
    - Is the data transferred to another country.
    - How long do you keep the personal data set (retention).
- The technical and organisational security measures to protect the personal data set.
- The legal basis for processing as described above (1).
- If consent is the legal basis for processing, details of the evidence of this consent.
- Put any risks found from the personal data processing audit process into a risk register.
- Review the school's consent forms so they meet the higher standards of UK GDPR, create an audit trail showing evidence of consent.
- Under 13's can never themselves consent to the processing of their personal data in relation to online services, this rule is subject to certain exceptions such as counselling services.
- Register with the Information Commissioners Officer as a data controller.
- Appoint a data protection officer who will monitor compliance with the UK GDPR and other data protection laws.
- Create a privacy notice that will let individuals know who we are, why we are processing their data and if we share their data.
- Create a system to allow data subjects to exercise their rights:
- Right to be informed via a privacy notice.
- Right of access via a subject access request within 1 month.
- Right of rectification to incorrect data within 1 month.
- Right to erasure unless there is a legal reason for processing their data.
- Right to restrict processing to the bare minimum.
- Right to data portability to receive their data in the format they request.
- Right to object to personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling.
- Amend any business contracts with suppliers to ensure that they will conform to new data protection legislation.
- Implement technical and organisational controls to keep personal data secure.
- Use Privacy Impact Assessments to assess the privacy aspects of any projects or systems processing personal data – please request a copy of our DPIA policy for more information
- Ensure an adequate level of protection for any personal data processed by others on behalf of the school that is transferred outside the European Economic Area.
- Investigate all information security breaches, and if reportable, report to the Information Commissioners Office within 72 hours.
- Undertake data quality checks to ensure personal data is accurate and up to date.
- Demonstrate our compliance in an accountable manner through audits, spot checks, accreditations and performance checks.
- Support the pseudonymisation and encryption of personal data.

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 when necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Rights of the Individual

The list of rights that a data subject (person who the data is about) can exercise has been widened by Section 2 of the UK GDPR:

- The right to be informed; via privacy notices.
- The right of access; via subject access requests (SARS), the timescale for response has been reduced from 40 calendar days to one calendar month. SARs must be free of charge, charges can only be made for further copies or where requests for information are unfounded or excessive.
- The right of rectification; inaccurate or incomplete data must be rectified within one month.
- The right to erasure; individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so.
- The right to restrict processing; individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future.
- The right to data portability; we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked.
- The right to object; individuals can object to their personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling; UK GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The school will ensure that these rights will be exercised.

Subject Access Requests

The school must provide a copy of the personal data to the data subject. In line with Article 15 of the GDPR, where the data subject submits an access request by electronic means, the information should be provided to the data subject by electronic means, unless otherwise requested by the data subject.

A SAR should be provided to the data subject free of charge. However, for additional copies provided to the data subject, the school may charge a reasonable fee or where access requests are “manifestly unfounded or excessive” taking into account the administrative costs of providing the information as outlined under Article 15 and Article 12 of the GDPR.

The school publishes on its website a Subject Access Request Form. The form gives information to data subjects about how to make a valid subject access request. Although requests can be made verbally, the school asks requests to me made in writing to ensure all information is provided and to ensure accurate records,

Special rules apply to subject access requests relating to information about the outcome of academic, professional or other examinations. These rules, which apply to requests for examination scripts, marks or markers’ comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body’s processes for announcing results.

Information comprising the answers given by a candidate during an examination is exempt from the right of subject access. A subject access request cannot be used to obtain a copy of an individual’s examination script.

Although this exemption does not extend to an examiner’s comments on a candidate’s performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded, there is a special rule governing the time limit for responding to a subject access request for such information in cases where the request is made before the results are announced. In such cases, a response must be provided within the earlier of:

- five months of the date of the request; and
- 40 days of the date on which the results are announced.

Where a subject access request is made for an individual’s examination marks, a response may only be refused (or delayed) for reasons permitted by the GDPR. So, it would not be appropriate to refuse to provide details of examination marks in response to a subject access request because the requester had failed to pay fees. Clearly, though, providing information about examination results is not the same as conferring a qualification.

Parents right of access to children’s educational record

Parents have a separate right of access to their child’s ‘educational record’ under ‘The Education (Pupil Information) (England) Regulations 2005. This right of access is only relevant to maintained schools – not independent schools, English academies or free schools. Whilst this right overlaps with subject access rights, the right to educational records is not dealt within this policy and procedure. Requests for pupil record will be handled in 15 school days in line with the legislation.

Exemptions

A subject access request may be refused where it is deemed “manifestly unfounded or excessive, in particular because of its repetitive character." The burden of demonstrating the manifestly

unfounded or excessive character will rest with the school as outlined under Article 12 of the GDPR.

There are other instances where the school may decide to refuse the request. Examples of reasons to refuse a request include where the requester is involved in a claim against the school, seeking compensation, and the information requested reveals details of the organisation's decision process in relation to their claim; or if releasing the personal data requested would mean that the personal data of another individual would be unfairly disclosed.

Children and subject access requests

Personal data about a child belongs to that child, and not 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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school will be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

When making a decisions as to whether those with parental responsibility can access their child's data, we will consider the following:

- The child's level of maturity and their ability to make decisions
- The nature of the personal data
- Any court orders in place relating to parental access or responsibility
- Any duty of confidence owed to the child
- Any consequences of sharing the information with those with parental responsibility, particularly in cases where there are allegations of abuse or mistreatment
- Any detrimental effect on the child if those with parental responsibility cannot access the information

Responding to a request

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual by 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
- May ask the individual to clarify their request

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Is exempt under any exemptions found in the UK GDPR and Data Protection Act 2018

Refusing a Request

Under Article 12 of the GDPR, where the school refuses to respond to a subject access request, the school shall inform the data subject without delay and at the latest within one month of receipt of the request of the following:

- Reasons for refusing to respond;
- The right to lodge a complaint with the Information Commissioner's Office;
- The right to seek a judicial remedy.

Deleting data

It is an offence under the GDPR to delete data that is the subject of an access request. Under no circumstances should the data be deleted even if it has been retained for a period longer than the school retention schedule permits.

Data Processors

Where the school uses a data processor, then it must notify the processor of the subject access request and ensure that contractual arrangements are in place to guarantee that such requests are dealt with efficiently by all data processors.

Data Breaches

Our Obligation

Where we become aware of a breach we will:

1. Assess whether the breach results in:
    - **No risk** to the rights in which case we do not need to notify the ICO or the data subject, e.g. an encrypted memory stick is lost, and the password has remained safe.
    - A risk to the rights and freedoms of the individuals, in which case we must notify the ICO within 72 hours, e.g. a spreadsheet of staff names and addresses is mistakenly sent by email to another school in the area. We should contact the headteacher of the school, who should confirm that they have deleted the email without reading it.
    - A **high risk** to the rights and freedoms of the individuals, in which case we must notify the ICO within 72 hours and the data subject without delay, e.g. a computer virus results in student data being accessible to hackers.
2. Communicate the breach to the ICO and where necessary the data subject.
3. Maintain a record of the breach. This includes breaches that do not require notification

Assessing the nature and risk from a data breach

The GDPR defines a breach in Article 4(12) as: *'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*

Breaches are categorised as:

(i) Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data

(ii) Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and

(iii) Integrity breach - where there is an unauthorised or accidental alteration of personal data

When assessing if a breach has a high impact we will consider:

- The category of data that is breached, i.e. are special categories of data included in the breach such as health records of students?
- The number of records breached, although even one record could result in a high-risk situation for the individual;
- The category of individual impacted by the breach, where children or vulnerable people are involved the risk is considered higher;
- The potential negative impact on the individual. High risk impacts include:

    - Identity theft
    - Fraud
    - Physical harm
    - Psychological distress
    - Humiliation
    - Damage to reputation;
- When in doubt as to the risk level we will notify the ICO and seek advice on the need to notify the individuals impacted.

Procedure for responding to data breaches

As part of our staff data protection training we make staff aware of what constitutes a data breach and of the need to inform the DPO/Headteacher in the event of a suspected breach.

In the event of a staff member becoming aware of a suspected data protection breach:

1. The staff member will inform the DPO/Headteacher;
2. The DPO/Headteacher will gather the relevant staff members to assess what has happened and the risk from the breach;
3. The DPO/Headteacher will document the breach
    a. Where necessary the DPO/Headteacher will notify the ICO as soon as possible (and not more than 72 hours from when the staff member became aware of the breach). The ICO has its contact information on the ICO website: phone 0303 123 1113.
    Where it is not possible to notify the ICO of all information immediately we will notify the ICO in phases as quickly as possible.
4. We will discuss the breach with the ICO and decide if we need to inform the data subjects;
5. Where necessary we will notify the data subjects
6. We will record the breach and keep a copy of this record.

Notification of breach to the ICO

In preparation for notifying the ICO we will document:

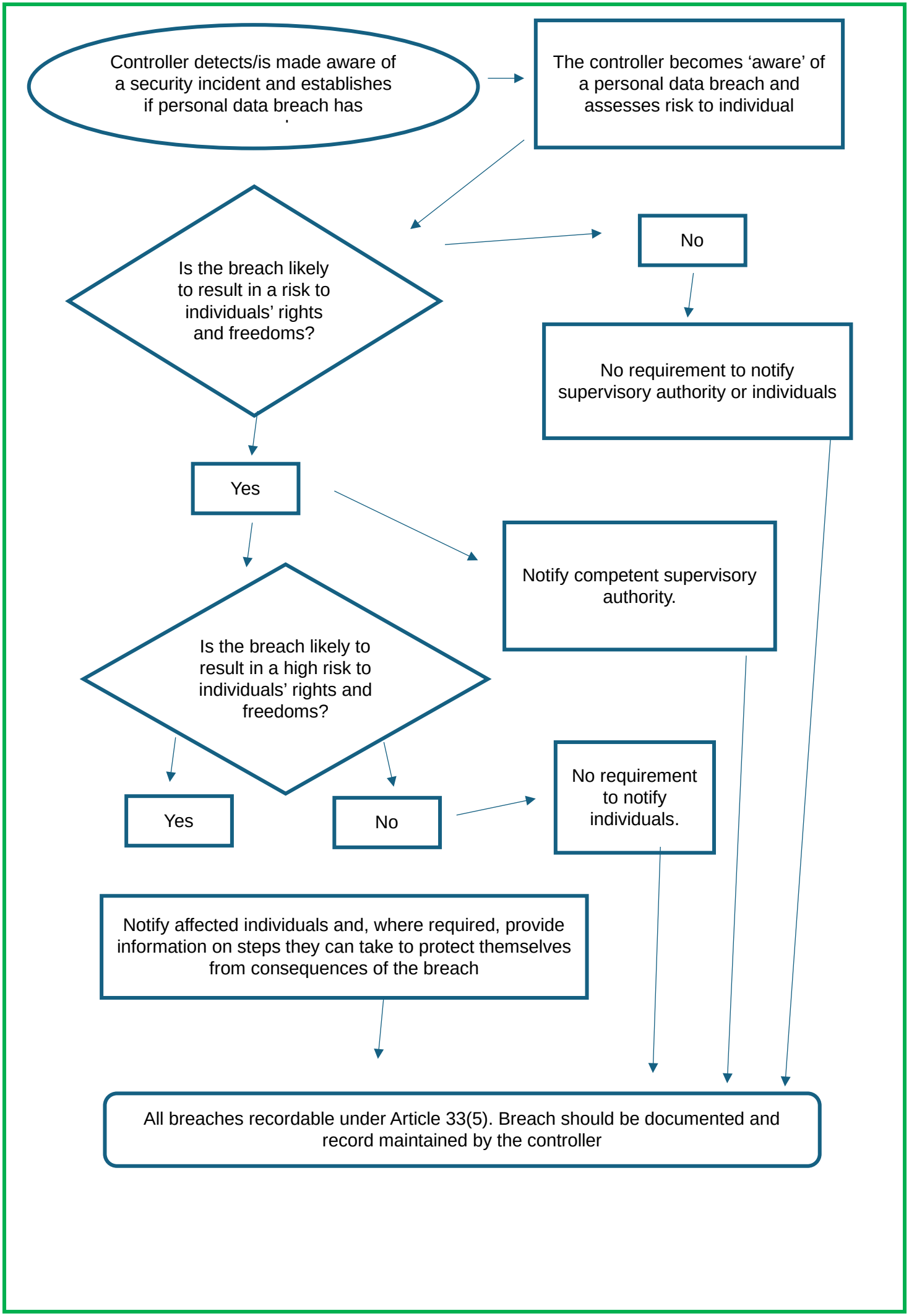
- What is the nature of the breach / what happened
    - Categories of data subject
    - Category of data
    - Type of breach
    - Number of records breached (to the best of our knowledge);
- The name and contact details of our DPO;
- The likely negative consequences of the data breach on the individuals impacted;
- Measures that will be taken by the school to mitigate the risk associated with the data breach. This will include immediate mitigating risks and longer-term plans to avoid a repeat of the breach.

We will communicate this information to the ICO. Where it needs to be communicated in phases we will not unduly delay the first notification

Notification of breach to the data subjects

In preparing for notifying the data subjects we will document:

- Some information on the breach that provides the individual with some detail and context;
- The name and contact details of our DPO;
- The likely negative consequences of the data breach on the individuals impacted;
- Measures that will be taken by the school to mitigate the risk associated with the data breach. This will include immediate mitigating risks and longer-term plans to avoid a repeat of the breach;
- Any advice that we can provide on what the individual can do to further reduce the risk to them.


Controller detects/is made aware of a security incident and establishes if personal data breach has
The controller becomes 'aware' of a personal data breach and assesses risk to individual
Is the breach likely to result in a risk to individuals' rights and freedoms?
No
No requirement to notify supervisory authority or individuals
Yes
Notify competent supervisory authority.
Is the breach likely to result in a high risk to individuals' rights and freedoms?
Yes
No
No requirement to notify individuals.
Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach
All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our grounds or whilst on trips and visits.
We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within the school on school notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as school photographers, newspapers, campaigns
- Online on our school websites 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 child, to ensure they cannot be identified.

Data Security and Storage of Records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the main office
- Passwords that are at least 8 characters long containing letters and numbers are used to access trust or school computers, laptops and other electronic devices. Staff and pupils are required to change their passwords at regular intervals and use multi-factor authentication where possible
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or Governors should not store personal information on their personal devices. Staff should use their own devices to do, or obtain prior consent from the ICT Support Team, should this be required for specific activities.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of Records

Personal data that is no longer needed will be disposed of securely and in line with our retention schedule. 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 GDPR regulation.

Working from home

Equipment needed to undertake occasional work from home will be IT equipment, internet and on occasions a telephone. The school will not provide IT equipment to employees unless it is part of their job role.

When working from home, the employee must be aware of the increased risk of a security breach. The employee must ensure that all documentation is stored securely, and that any laptop or iPad is password protected and turned off when not in use. If a security breach occurs, then the employee must refer to the data breach procedure and report the breach immediately.

Employees are not permitted to store any personal data relating to the trust on their personal devices and should take note of the good working practices listed below:

- When working from home, the employee must be aware of the increased risk of a security breach. The employee must ensure that all documentation is stored securely, and that any laptop or PC is password protected and turned off when not in use.
- Do not engage in activity that threatens the integrity of the school systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Under no circumstance are users allowed to download any software or obscene material using the internet.

Training

All Euxton Primrose Hill staff are trained to be aware of their responsibility to report subject access requests as quickly as possible. They will also be made aware of the procedure for responding to subject access requests and the point of contact to which subject access requests are required to be reported. This is likely to be the School's Data Protection Officer in most instances.

The school expects its staff to comply with its data subject access request policy and procedures in full. Any breach of this policy may result in disciplinary action against the individual in accordance with its procedures.

Review and related policies

This policy is in conjunction with the following:

- Freedom of Information Policy and Publication Scheme
- Records Management Policy and Retention Scheme

- Privacy Notices
- DPIA Procedure

Contact

Contact the Data Protection Officer by:

Email: bursar@primrosehill-euxton.lancs.sch.uk

Phone: 01257 276688 or

Post: Euxton Primrose Hill Primary School, Primrose Hill Road, Euxton, PR7 6BA

Version Control

Named Owner:	Mrs Joanne Vost – Data Protection Officer
Version Number:	5.00
Date Of Creation:	May 2018
Last Review:	October 2024
Next Scheduled Review:	October 2025
Overview of Amendments to this Version:	Data Breach Policy and Subject Access Request policy integrated, additional information