Data Protection- Breach, retention GDPR & Asset Management Policy

Policy Originator	Lisa Rawashdeh
Governor Responsible	Tom Spencer
Ratified on	16.11.20
Review period	Annual (Autumn '21)

Policy Origin	**Haringey**
Changes since last version	**No Changes**

DATA PROTECTION POLICY

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Ferry Lane Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Ferry Lane Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Ferry Lane Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has four Designated Data Controllers: They are the Admin Officer (SM) Admin Manager (SH), the Head teacher (NM) & the Acting Deputy Head teacher (HC).

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be:
The Head teacher

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently.

The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

If and when, as part of their responsibilities, staff collect information about other people(e.g. about a pupil's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools Data Protection Code of Practise.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practise address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to Mr Sam Hall - administrator.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent

In many cases, the School can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of

personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job.

The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users.

The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy.

Because this information is considered **sensitive** under the 1998 Act, staff (and pupils where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Retention of Data

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts.

Different categories of data will be retained for different periods of time.

Data Protection Officer

The School has procured the services of Judicium, who provide a Data Protection Officer and relevant services/support. The Data Protection Officer is responsible for

overseeing data protection within the School and can be contacted on the information below: -
Data Protection Officer: Craig Stilwell
Company: Judicium Consulting Ltd
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

DATA BREACH POLICY

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Definitions

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Personal Data Breach

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

Data Subject

Person to whom the personal data relates.

ICO
ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

Responsibility

Lisa Rawashdeh has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of **Lisa Rawashdeh**, please contact **Sam Hall**.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

Security and Data-Related Policies

Staff should refer to the following policies that are related to this data protection policy: - GDPR Policy which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.

Data Protection Policy which sets out the School's obligations under GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found in the public drive or on the school's website.

Data Breach Procedure

What Is A Personal Data Breach?

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

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

When Does It Need To Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form (which can be obtained from **Sam Hall**);
- Email the completed form to **Lisa Rawashdeh**.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, **Sam Hall** or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. **Lisa Rawashdeh** will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording The Breach

On being notified of a suspected personal data breach, **Lisa Rawashdeh or Sam Hall** will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notifying the ICO

Lisa Rawashdeh will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, **Lisa Rawashdeh or Sam Hall** will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, **Lisa Rawashdeh or Sam Hall** will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;

- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing The Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether its necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to

Lisa Rawashdeh, Sam Hall or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

Primary GDPR Policy

The General Data Protection Regulations

Policy Originator	Lisa Rawashdeh
Governor Responsible	Catherine Nicholls
Ratified on	16.11.20
Review period	Annual

Contents

1. Purpose

1.1 The Data Protection legislation (The General Data Protection Regulations (GDPR) and the Data Protection Act 2018) protect individuals with regard to the processing of personal data, in particular by protecting personal privacy and upholding an individual's rights. It applies to anyone who handles or has access to people's personal data.

1.2 This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018). It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2. Scope

2.1 The GDPR and DPA 2018 have a wider definition of personal data than the Data Protection Act 1998 and includes information generated from cookies and IP addresses if they can identify an individual.

2.2 'Personal data' is any information that relates to an identified or identifiable living individual, which means any living individual who can be identified, directly or indirectly, in particular by reference to—

a. an identifier such as a name, an identification number, location data; or
b. an online identifier; or
c. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3 The DPA 2018's wider definition of personal data also includes any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV) or sound recordings.

2.4 The processing of personal data for must be lawful and fair. Under the DPA 2018 "sensitive processing" means the processing of personal data revealing information on an individual that falls under the following:

- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data;
- Health;
- Sex life;
- Sexual orientation.

2.5 This School collects and a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data.

2.6 The School may also be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies (e.g. Department of Education) and other bodies.

2.7 To comply with the Data Protection legislation, this School will collect, use fairly, store safely and not disclosed personal data to any other person unlawfully.

3. General Data Protection Principles

3.1 The School needs to demonstrate compliance with six core principles governing processing of personal data:

a. Processing of data is lawful and fair;
b. Purpose is specified, explicit and legitimate (Purpose limitation);
c. The personal data be adequate, relevant and not excessive (Data minimisation);
d. Date processed is accurate and kept up to date (Accuracy);
e. Personal data be kept for no longer than is necessary (Storage limitation);
f. Personal data is processed in a secure manner (Integrity and confidentiality).

3.2 Under the DPA 2018, the wider territorial scope means that the Regulations apply to any Personal Data of any individual who is located in an EEA country irrespective of the country or territory of the organisation processing the data.

3.3 The School will therefore ensure that its contracts with organisations that may process personal data on its behalf are compliant with the Regulations and offer adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Lawful processing

4.1 The School must have a valid lawful basis in order to process personal data.

4.2 The six lawful basis for processing personal data are:

(a) Consent: the individual provides clear consent to process their personal data for a specific purpose;
(b) Contract: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose, for example, staff employment contract or pupil placement;
(c) Legal obligation: the processing is necessary for the School to comply with the law (not including contractual obligations);
(d) Vital interests: the processing is necessary to protect someone's life;
(e) Public task: the processing is necessary for the School to perform a task in the public interest/official functions, and the task or function has a clear basis in law;
(f) Legitimate interests: the processing is necessary for a legitimate interests or the legitimate interests of a third party unless there is a good reason to

protect the individual's personal data which overrides those legitimate interests.

4.3 The School will generally rely on the following three legal bases for processing data as follows:

(a) Consent;
(b) Contract;
(c) Legal obligation.

4.4 The School will detail its lawful basis for processing personal data in its privacy notice(s).

5. Roles and Responsibilities

Employees

5.1 Every employee, staff member or worker that holds personal information on behalf of the School has to comply with the Data protection Act when managing that information and must treat all personal data in a confidential manner and follow the guidelines as set out in this document.

5.2 All members of the school community are responsible for taking care when handling, using or transferring personal data.

5.3 All members of the school community has a responsibility for ensuring that data cannot be accessed by anyone who does not have permission to access that data.

5.4 Data breaches can have serious effects on individuals and institutions concerned and can bring the School into disrepute. Members of the School community who breach this Policy and/or the Data Protection legislation will be subject to disciplinary action under the School's Disciplinary Policy, which can include sanctions up to and including dismissal. Such breaches may also lead to criminal prosecution.

Pupils over 13 years of age

5.5 Under the DPA 2018, Children aged 13 or over are able to provide their own consent for the processing of their personal data.

5.6 When a child attains 13 years of age, the School will rely on the consent previously provided by the parent(s)/Legal Guardian(s) of the individual.

5.7 If a pupil aged 13 or older wishes to revoke or change the consent previously provided by the pupil's parent(s)/Legal Guardian(s), the individual must suggest and agree with the School a specific agreement on how their data is to be processed.

5.8 Where a pupil is not able to suggest or agree a specific arrangement with the School on how their data is to be processed, the School will continue to process the pupil's

data under the parent(s)/legal guardian(s) previously provided consent. The School will inform the pupil of this decision.

5.9 When processing personal data the School will think about the need to protect pupils from the outset, and will consider privacy in its systems and processes during the design stage.

The School - Responsibilities to all data subjects

5.10 The School will ensure that it manages and processes personal data properly; and that protects an individual's right to privacy.

5.11 On request, the School will provide an individual with access to all personal data held on them under a Subject Access Data Request.

5.12 The School has a legal responsibility to comply with the DPA 2018 and the GPDR. The School, as a corporate body, is named as the Data Controller under the DPA 2018.

5.13 The School will consider privacy at the outset and use a data protection by design and by default approach.

5.14 The School will not exploit any imbalance in power in the relationship between the School and its data subjects.

5.15 The School is committed to ensuring that its staff are aware of data protection requirements and legal requirements and will raise awareness of the importance of compliance.

5.16 The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

The School - Responsibilities to Pupils

5.17 As a matter of good practice, this School will use Data Protection Impact Assessments (DPIA) to help assess and mitigate data privacy risks to children.

5.18 Where the School processes data that is likely to result in a high risk to the rights and freedom of its pupils it will always complete a DPIA.

5.19 As a matter of good practice, the School will consult with children aged 13 and over as appropriate when designing its processing.

5.20 If the School relies on consent as the lawful reason for processing data it will ensure that children aged 13 or over understand what they are consenting to. The reasons for lawful processing will appear in the School's Privacy Notice.

5.21 When relying on 'necessary for the performance of a contract' as its the lawful reason for processing the School will consider the child's competence to understand what they

are agreeing to, and to enter into a contract. Where the School believes that a child's competence prohibits informed consent, the School will inform the child of the intention to obtain consent from the child's parent(s)/legal guardian(s). The School will only allow competent children to exercise their own data protection rights.

5.22 Subject to Section 6 below, where the School has relied on consent that was provided by the parent(s)/Legal guardian(s) of the child; when the individual attains 13 years of age the school will comply with request for erasure whenever it can.

5.23 When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Governors

5.24 Governors are responsible for monitoring the School's compliance with the Regulations.

5.25 Governors may periodically review the DPIAs to assess the School's compliance with the Data Protection legislation.

6. Photographs, video and CCTV images

6.1 Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

6.2 Unless prior consent from parents/pupils/staff has been given, the School shall not utilise such images for publication or communication to external sources.

6.3 It is the School's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

7. Data Security

7.1 The School will use proportionate physical and technical measures to secure personal data.

7.2 The School will consider the security arrangements of any organisation with which data is shared shall and where require these organisations to provide evidence of the compliance with the DPA 2018 and GDPR.

7.3 The School will store hard copy data, records, and personal information out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. These will be stored in the main office and the secured staffroom.

7.4 Sensitive or personal information and data should not be removed from the school site, however, the School acknowledges that some staff may need to transport data

between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

7.5 To reduce the risk of personal data being compromised any individual taking personal data away from the School site must adhere to the following:

7.5.1 Paper copies of personal data should not be taken off the school site as if misplaced they are easily accessed. If no alternative is available other than to take paper copies of date off the school site then the individual must ensure that the information should not be on view in public places, or left unattended under any circumstances.

7.5.2 Unwanted paper copies of data, sensitive information or pupil files must be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

7.5.3 Individuals must take care to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

7.5.4 Where information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

7.5.5 Teaching Staff must ensure that personal data and sensitive personal data is not displayed inadvertently on White Boards during class lessons.

7.5.6 If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only. USB sticks that staff use must be password protected.

7.5.7 Breaches of the policy will be dealt with in accordance with the School's disciplinary policy and could amount to gross misconduct.

8. Data Retention and Disposal

8.1 The School does not retain personal data or information for longer than it is required, however it is recognised that the School will retain some information on employees and pupils after individuals have left the School.

8.2 The creation of systems and/or files, which duplicate such data will be avoided; where it is inevitable every care will be taken to ensure that data maintained in secondary systems is accurate and kept up to date. Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

9. Data Impact Assessments

9.1 The School will conduct assessments to understand the associated risks of processing personal data that it gather/intends to gather to assist in assuring the protection of all data being processed. The School will use these assessments to inform decisions on processing activities.

9.2 Risk and impact assessments shall be conducted in accordance with guidance given by the ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

10. Data Subjects right to be forgotten – Data Erasure

10.1 Data Subjects have the right to request the erasure of their personal data. The School will not comply with a request where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

10.2 The School will design its processes so that, as far as possible, it is as easy for a data subject to have their personal data erased as it was for the individual to give their consent in the first place.

11. Data Access Requests (Subject Access Requests)

11.1 All individuals whose data is held by the School, have a legal right to request access to such data or information about what is held. No charge will be applied to process the request.

11.2 Requests must be made in writing to the Data Protection Officer and the School will respond to within one month of receiving the request.

11.3 Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following organisations without consent:

Other schools

11.3.1 If a pupil transfers from Ferry Lane Primary to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school.

11.3.2 This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation, which should ensure that there is minimal impact on the child's academic progress because of the move.

Examination authorities

11.3.3 This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

11.3.4 As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts

11.3.5 If a situation arises where a criminal investigation is being carried out, the School may have to forward information on to the police to aid their investigation. The School will pass information onto courts as and when it is ordered.

Social workers and support agencies

11.3.6 In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division

11.3.7 The School may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

11.3.8 The Data Protection Officer is: Craig Silwell, Judicium

12. Breaches

12.1 The School will notify the individual and the ICO of breaches of personal or sensitive data within 72 hours of becoming aware of the breach.

13. Notifying the Information Commissioner

13.1 The School is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link : http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

14. Further information

14.1 Additional information on the School's Data Protection obligations is located in its Privacy Notice(s).

14.2 The Data Protection Officer is available to provide advice on this policy and information on how the School applies the GPDR and Data Protection Act. See Section 11.3.8 above for the contact details of the DPO.

DATA RETENTION POLICY

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

DATA PROTECTION

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's Data Protection Policy outlines its duties and obligations under the GDPR.

RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by **Sam Hall**.

Electronic records will be regularly monitored by **Sam Hall**.

The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

DESTRUCTION OF RECORDS

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by **Sam Hall**. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

TRANSFERRING INFORMATION TO OTHER MEDIA

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

RESPONSIBILITY AND MONITORING

Sam Hall has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The data protection officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	2 years after employment ceases
Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel and training records	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: • Opt out forms • Records of compliance with WTR	• Two years from the date on which they were entered into • Two years after the relevant period
Disciplinary and training records	6 years after employment ceases
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.

Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	No longer than necessary
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
School Development Plans	3 years from the life of the plan
Professional Development Plans	6 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Newsletters and circulars to staff, parents and pupils	1 year
Health and Safety Records	
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	3 years from the life of the risk assessment
Any reportable accident, death or injury in connection with work	For at least twelve years from the date the report was made
Accident reporting	Adults – 6 years from the date of the incident Children – when the child attains 25 years of age.
Fire precaution log books	6 years
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record

Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Pupil Records	
Admissions records	1 year from the date of admission
Admissions register	Entries to be preserved for three years from date of entry
School Meals Registers	3 years
Free School Meals Registers	6 years
Pupil Record	Retained while the child is at the school. Sent to new school upon leaving
Attendance Registers	3 years from the date of entry
Special Educational Needs files, reviews and individual education plans (this includes any statement and all advice and information shared regarding educational needs)	Until the child turns 25.
Emails	
General emails in staff accounts (where emails pertain to a previous category, i.e. they contain SEN information, they should be retained according to the appropriate retention period for that category)	2 academic years
Other Records	

Asset Management Policy

1. INTRODUCTION:

1.1.1 The Governing Body of Ferry Lane Primary School is responsible for the proper management and security of the school premises and the custody and physical control of all other assets including machinery, furniture, equipment, stock and other assets such as cash.

1.2 The Asset Register

1.2.1 Ferry Lane Primary School maintains an Asset Register of items held by the school that the Governing Body deems to be valuable and/or subject to an insurance claim. Moveable assets valued at £1000.00 or more must be recorded. Note that all Information Technology (IT) equipment must be recorded, regardless of their value.

1.2.2 The Asset Register should include the following information:

- Date of acquisition of asset
- Description of asset, including colour, a unique identification mark such as serial number and security marking, where appropriate
- For ICT/electrical equipment, a record of the model or other unique reference/security number
- Cost of the asset purchased
- Source of funding
- Location of the asset
- Details of the disposal of any assets, whether scrapped, sold or donated
- Details of the revaluation of an asset
- Items used by the school but owned by others (eg leased items) supported by a note of ownership

1.2.3 Where possible, the Asset Register should be held within the school's financial system, rather than as a hardcopy document.

1.2.4 A copy of the Asset Register must be kept in a safe, fireproof place, and be available for inspection.

1.2.5 Acquisitions and disposals should be recorded on the register at the time of acquisition or disposal and reported to the Governing Body.

1.2.6 The Governing Body must ensure that the asset register is kept-up-to-date and is reviewed at least once a year. The review must include the physical check of the assets and must be performed by someone other than the person maintaining the register. The asset register should be certified and dated on completion of the review.

1.2.7 The upkeep of the asset register can be particularly important for insurance reasons, as policies will often limit the insurance of equipment etc to those items present on the school asset register.

1.2.8 Register should be reconciled annually with the School's Insurance Services records. Where the school participates in the Council's insurance programme, the register submitted to the Council should contain all audio/visual/ICT items.

1.3 Loaning Assets

1.3.1 An asset can be loaned to staff of the school, and Ferry Lane must keep a log of such loans. Where a loan of asset could be deemed a benefit in kind and therefore have tax implications for the individual, the relevant paperwork must be completed.

1.3.2 Staff wanting to loan an asset must report to the Admin Officer to complete an equipment loan form. This will include all details of the loaned asset and needs to be signed by an authorising staff member (Admin Officer or Head Teacher).

1.3.3 Upon the ending of the loan period the staff member should return the item to the Admin Officer who will confirm receipt of the item. Both the staff member and an authorising staff member should sign the equipment loan form to confirm the asset has been returned.

1.4 **Disposing of Assets**

1.4.1 The Governing Body of Ferry Lane may dispose of assets through sale, donation or scrapping.

1.4.2 Assets that have been disposed of must be removed from the Asset Register, and the insurer notified.

1.4.3 For every disposal, the Governing Body or the person who is maintaining the Asset Register must: - Record the reasons for the disposal - Be able to demonstrate that the assets are either obsolete or surplus to requirements

1.4.4 Head teacher must appoint a single person to be responsible for disposing of assets, and inform them in writing that they are ultimately accountable for doing so. The responsible person's name must be clearly identified in the school's disposal file. (Sam Hall, Admin Officer)

1.4.5 Any disposal of a capital asset must be made in accordance with the school's policy on purchasing and disposal and, where the disposal involves land and/or buildings funded by the LA, the school must obtain formal advice and approval from the local authority Haringey.

1.4.6 Ferry Lane Primary School must ensure that they adhere to the latest WEEE (Waste Electrical and Electronic Equipment) Legislation, which sets out the requirements for disposing of electrical/electronic equipment, (see http://ec.europa.eu/environment/waste/wee/legis_en.htm). The legislation states that such assets cannot just be thrown away, must be disposed of properly, either by: - Donation to a charity (for refurbishment and re-use) – eg Tools for Schools - Disposal by a specialist organisation, who will take such items away and recycle them.

1.4.7 Before disposing of computer equipment school must ensure compliance with Data Protection Act 1984 by erasing all personal data from the hard disk. Note that merely deleting files may not physically remove the data, which could be restored using specialist products. School must also ensure that any software products for which licences are maintained in-house are removed from the equipment prior to disposal.

1.4.8 Any member of staff who determines that an asset is surplus to requirement, or who is involved in the disposal, should never attempt to purchase it or take it for personal gain. There should be a clear separation of duties and the Head teacher must approve all disposals.

1.4.9 Official receipts must be issued for income received for disposed assets. Monies must be received and properly accounted for by someone who has not been involved in the disposal.

1.4.10 The income received from the sale of any asset must be treated as income in the school's budget, unless it relates to the sale of certain assets (such as land and buildings owned by the LA) or to income from a Public/Private Partnership (PPP) or Private Finance Initiative (PFI), which are subject to a specific agreement.

1.5 Obsolete Assets

1.5.1 Assets are deemed obsolete if they have no resale value.

1.5.2 Ferry Lane Primary School may donate surplus, obsolete assets to the voluntary sector or scrap them.

1.6 Surplus Assets

1.6.1 Where the possible sale value for an item or group of items exceeds a predetermined threshold value, the school should seek to dispose of them by quotation, competitive tender or public auction, unless approved by the Governing Body to do otherwise.

1.6.2 The threshold value should be set by the Governing Body

1.7 Retention of Disposal Documentation

1.7.1 All documentation relating to the disposal of the asset must be retained for a period of six years after the disposal.

1.7.2 The following types of document should be retained: - The Governing Body or Head teacher's written record declaring the asset surplus, and instructions to the person appointed as responsible for the disposal - The advertisement - The offers made - The receipt

1.8 Security – General

1.8.1 The Governing Body is responsible for the security of the school's assets.

1.8.2 It is the responsibility of all Budget Holders to ensure that a yearly stock check is carried out during the summer term. Any missing items must be reported to the Governing Body.

1.8.3 Appropriate arrangements must be in place for the security of all assets. Security measures could include the following: - Secure equipment and other assets by means of physical and other security devices (eg locked in cupboards) - Authority to access these secured assets should be clearly documented - All items in the asset register should be permanently and visibly marked as the school's property - Maintain a record of any model or other unique reference/security number in the asset register - Clearly mark any portable equipment that is vulnerable to theft with the name of the school

1.8.4 Items which are easily portable and saleable (videos, televisions, computers, cameras, etc) must be security marked and kept securely locked away when not in use, particularly overnight. Keep a separate record (in the Asset Register) of any model or other number unique to your machines.

1.8.5 Items of school property should not be removed from the school premises without the appropriate delegated authority.

1.8.6 Should property be removed from the school premises, the school should: - Establish the position related to insurance before the assets are taken off site - Be aware that assets on loan for extended periods or to a single member of staff on a regular basis may be deemed a benefit-in-kind, which may be subject to taxation - Keep a record of all assets removed from the school premises - Update the record when the assets are returned

1.9 Computer Security and Protection

1.9.1 School computer systems hold sensitive financial and personal data. School must, therefore, take appropriate action to ensure that equipment and data is kept secure.

1.9.2 School should have a written ICT Security Policy, which should encompass the guidelines for protecting hardware and software, set out below.

1.10 Protecting Hardware

1.10.1 The main dangers to hardware are: - Loss through theft - Damage (accidental or otherwise)

1.10.2 To minimise the danger of loss or damage, the machines should be:

- Labelled with a unique asset number

- Entered onto the school's asset register with their serial numbers

- Correctly positioned (ie towers not laid on their sides)

1.10.3 If possible, the machines should also be:

- Not visible from outside the building or to the public generally

- Kept in a locked room when not in use, particularly overnight

- Where possible, secured to furniture

- Labelled, marked with indelible pen or have the name of the school soldered onto the case

1.10.4 To minimise damage and the chances of the machines being damaged all users should:

- Refrain from eating or drinking whilst working on the machines

- Never move or attempt to clean a machine without first obtaining the IT co-ordinator's advice

- Ensure any loose cabling into the machine is not in danger of being stood on or tripped over by staff

- Know who to contact in the event of a breakdown of the machine

1.10.5 Laptops and other easily portable equipment are particularly vulnerable to theft and damage. They should be kept in a locked cupboard when not in use and carefully protected when taken outside the office.

1.10.6 File servers must be kept in secure rooms, with access limited only to authorised individuals.

1.11 Protecting Software

1.11.1 The main danger to software are:

- Unauthorised access to data

- Accidental loss of data by the user or because of machine failure

- Corruption of data by computer viruses

1.11.2 To minimise the danger of unauthorised access, users should ensure that:

- The system is returned to the password screen when leaving the office

- The machine is switched off when not in use

1.11.3 Only authorised staff should have access to computer hardware and software for the school management.

1.11.4 Passwords should be used to stop unauthorised access to information.

1.11.5 Procedures should also exist for a new password to be issued to new staff, and withdrawn when staff leave.

1.11.6 Passwords should be:

- At least six characters long and preferably contain a number

- Changed regularly (every 90 days) and as soon as a user leaves

- Not shared between users

- Not written down

- Not obvious (such as the user's telephone number)

1.11.7 School should have a recovery plan in the event of loss of accounting or financial data. The plan should outline the need for and frequency of electronic back-up, secure storage back-ups (if possible, off-site), and manual procedures to provide support for key processes where normal system usage is not possible.

1.11.8 The following precautions should be taken to minimise any loss of data caused by machine failure or user error. (When PCs are networked and data is stored to a server, these functions should be carried out by the System Administrator)

- Give all users proper written instructions on how to use the system

- Back up all data regularly (ie files created by the user such as word processor documents or spreadsheet files). It is recommended that data be backed up after 8 hours' work on the machine

- If possible, keep at least three generations of back-up (ie the previous three back-ups). Back-up cycles should be taken daily, weekly and monthly

- Maintain a back-up of all operating software (such as Windows NT)

- Store the system disks/CDs for the applications (such as Microsoft Office) securely

- Store all back-ups away from the vicinity of the machines in a fireproof, locked cabinet or safe-preferably off-site

- Ensure that there is adequate hardware maintenance cover for critical equipment

1.11.9 To minimise the danger of data corruption by viruses and an-antivirus solution must be implemented for all networked PCs and servers. There is a continuing threat from previously undetected viruses, so staff should take the following precautions:

- Never load software without the school's IT co-ordinator's approval, including software from the internet.

- Never load any disks/CDs sent unexpectedly through the post (for example, demonstration or customer research software)

- Strictly control the transfer of software and data from one machine to another

- Never make unauthorised copies of any software

- Ensure virus-checking software is installed on all computers, and regularly updated

1.12 Unauthorised Use of Software and Data Protection

1.12.1 The 7th Data Protection Principle of the 1998 Act requires personal data to be surrounded by proper security. Take care at all times to ensure that staff does not render themselves liable to prosecution under the Data Protection Act.

1.12.2 Take particular care to protect data accessed or processed by 3rd parties. Any contract held with organisations or contractors authorised to process Council data should specify the security standards required. Advice on how to comply with the Act is available from Haringey's IT team under service level agreement arrangements.

1.12.3 Unauthorised copying of software is illegal under copyright.

1.13 Internet Usage

1.13.1 Web filtering should be installed to automatically block any inappropriate websites from being accessed.

1.14 Computer Printouts

1.14.1 Employees must not release information or computer data, particularly that of a personal or sensitive nature, to unauthorised persons.

1.14.2 Take care to prevent inadvertent disclosure of information, eg by ensuring that paper is suitably filed and disposed of securely.

1.14.3 Confidential waste must be shredded.

1.15 Further Advice

1.15.1 Staff in Haringey's IT Division can provide advice under service level agreement arrangements, if required. Haringey IT Help