FHS
Francis Holland Schools

Data Protection Policy

This policy applies to:

Francis Holland Regents Park Francis Holland Sloane Square Francis Holland Prep

Where there are differences between the schools these have been clearly highlighted.

Policy owner	Trust: Director of Information Systems
Type of policy	Regulatory [Regulation number: Part 1 3(g) GDPR
Last reviewed / approved by / date	SLTs: November 2024 Governance and Nominations: 6 February 2024
Next school review due	Autumn 2024
Next council review due	Spring 2025
This version published	April 2024
Circulation	☐ Trust Website ☐ Schools' Websites ✓ Schools' Sharepoints ☐ FHS People All policies are available from the Trust Office, Francis Holland Schools Trust, 35 Bourne Street, London, SW1W 8JA
Linked Policies	Expulsion and Required Removal

Revision History
This section should be completed by the reviewer each time this policy is reviewed

Changes made [Brief description of edits]	Date
Minor word changes to reflect our switch to use of cloud storage as the primary way of remotely accessing data instead of the remote desktop platform.	15/11/2021
Six-month data retention policy for emails removed as it is not applicable to school environments	14/01/2022
Updated references from GDPR 2018 to UK GDPR. Updated contact information of DPO. Added section on Subject Access Request and how to make a request via Judicium.	23/11/2023
Addition of section on data breach [approved at Governance and Nominations 4/6/24]	05/06/24

Data Protection

Introduction

Francis Holland Schools Trust, its Schools and staff, herein referred to as the **Trust**, are committed to treating personal data in a responsible, open and trustworthy manner, which maintains compliance with data protection laws.

Applicable Regulations and Laws

This policy takes into account the Trust's obligations in line with the following legal and regulatory mechanisms:

- The Data Protection Act 2018
- UK General Data Protection Legislation (UK GDPR)
- The Privacy and Electronic Communications Regulation 2011
- The Protection of Freedoms Act 2012
- Joint Council for Qualifications – General Regulations for Approved Centres

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

Terminology

- **Personal data** – is any data relating to a living individual (i.e. staff, pupils, parents/guardians and third parties).
- **Special categories of personal data (sensitive personal data)** – is a category of personal data which is subject to additional regulation. It is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health, sex life or sexual orientation, genetic data, or biometric data for uniquely identifying someone.
- **Data controller** – decides on how personal data is used and for what purpose. Holds primary legal responsibility and accountability for the protection of personal data.
- **Data processor** – does something with the data, including recording, collecting, storing and analysing.
- **Breach** – is anything leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Data Protection Officer (DPO)*** – is the Trust's primary point of contact for data protection officer duties. The DPO liaises with the Information Commissioner's Office (ICO), monitoring and reporting on compliance.

  **This terminology is used for convenience; however, the Trust does not employ an officially titled DPO.*

Both **Personal Data** and **Special Categories of Personal Data** (Sensitive Personal Data) will be referred to as **Personal Data** in this policy.

Data Controller

The Trust is the Data Controller under the UK General Data Protection Legislation (UK GDPR) and the Data Protection Act 2018.

Data Processors

The Trust is a Data Processor under the General Data Protection Regulation 2016 and the Data Protection Act 2018. The Trust also employs various third parties as Data Processors. Data subjects must be notified where such a processor is used and this engagement will be covered by a contractual agreement ensuring that data protection maintained.

Data Protection Officer (DPO)

The Trust's designated DPO can be contacted as follows:

Judicium Consulting Ltd
72 Cannon Street
London
EC4N 6AE
dataservices@judicium.com
0345 548 7000

Principles

The Trust follows these regulatory principles. Personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Trust, as a Controller is:

- responsible for, and must be able to demonstrate, compliance with the above principles.

Personal Data Processing

The Trust processes personal and other types of data in pursuit of its responsibilities as an education centre, including admissions, governance, management, academic, pastoral, safeguarding, co-curricular, development and alumni duties. Where applicable, explicit consent must be obtained for additional processing duties. The Trust also has legal and regulatory obligations, which require the additional processing of personal data. The Trust may receive and share relevant personal data in the form of references and applications for continued education.

The Trust directly or indirectly processes personal data about past, current and prospective pupils, parents, staff, contractors and other individuals who interact with it, including but not limited to the following data types:

- Contact details.
- Financial details (i.e. for billing and payments).
- Academic, pastoral, behaviour, attendance and activity records.
- Medical information.
- Incident records.
- Special education needs information.
- References.
- Communication and meeting records.
- Images.
- CCTV footage.

Third Parties and Cloud Providers

The Trust may engage third party processors and cloud service providers for services such as email, backups, online trip payments, ticketing platforms, counselling, management information systems, development initiatives and communications.

Applicable data subjects must be notified of any third party processors via data collection privacy notices.

Staff must only use third parties approved by the DPO and any such engagement must be subject to a contractual agreement ensuring compliant levels of data protection.

The Trust must not process or use any third party processor involving transferring personal data outside the European Economic Area (EEA) without explicit consent or suitable legal mechanisms.

Disclosure Exemptions

The Trust can disclose personal data without notification under certain instances, including:

- Data subject consent.
- National security interests.
- In the prevention or detection of a crime.
- To prevent serious harm (safeguarding).
- Legal and regulatory obligations.
- In connection with legal proceedings or advice.

Processing Guidelines

The Trust and its staff must always ensure that processing activities are compliant with the principles and rules of data protection regulations. If in any doubt, advice must be sought from the DPO.

This section covers core-processing rules that all staff must follow to ensure adequate levels of data protection are maintained.

- Personal data must be kept for limited periods of time, in accordance with the Trust's Data Retention Schedule (see **Appendix I**). Once a record has reached its retention limit, electronic versions must be deleted and physical copies destroyed and disposed of.
- Electronic records including personal data must be saved within management information systems or the relevant storage areas. Duplicates must be avoided.
- Paper records must always be filed in locked storage.
- Staff should avoid using emails to store personal data. Links to shared files should be used wherever possible, instead of attachments.
- Personal data records must not be on display in public areas (with exception of certain Junior School medical alert documents).
- All offices, staff rooms and staff only areas where personal data is kept, must only allow access through a lockable door. This must be kept locked when unattended or otherwise appropriate.
- Where personal data is emailed or stored online, the school provisioned email and cloud storage platforms must be used, unless otherwise approved by the DPO.
- Cloud services must be approved by the DPO before use.
- Teacher markbooks/planners remain the property of the Trust.
- Teacher markbooks/planners must employ a personal or the relevant school coding system to indicate any medical, special education needs or personal data other than academic performance records.
- Contact information cannot be stored in markbooks/planners.
- Electronic markbooks/planners must be approved by the DPO before use.
- Electronic markbooks/planners must have an export function.
- Marks are pupil data and must be uploaded onto school systems at least once per term.
- Any service which stores or transfers data outside the EEA must not be used.
- Usage of USB storage with personal data is strongly discouraged and cloud storage should be used instead. Where unavoidable, encrypted USB storage must be used.
- All school mobile devices must have encryption enabled.
- Staff must use cloud storage or remote access platforms if working with data offsite. Where unavoidable, limited personal data can be processed by staff on personal devices in support of schoolwork. However, these devices must be password protected, ideally encrypted and the data must be erased immediately after use. Special categories (sensitive) of personal data must never be processed on personal devices.
- Personal data that is to be taken offsite, such as for residential trips, must primarily be stored electronically on a school mobile device. A backup physical copy of the required data can be taken and must be kept secure.
- Pupil images can only be used for purposes other than internal identification and security with explicit consent.

Data Subject Rights

Data subjects have the following rights:

- The right to be informed.
- The right of access.

- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Some of these rights are absolute and others are dependent on other factors.

- Staff must forward requests to exercise any of these rights to the DPO within one working day.
- The DPO may need to ask staff to supply information to fulfil a request. Staff must respond to any such data protection requests within three working days.
- The DPO must respond to data subjects who have made a rights request within twenty five days (thirty days is the regulatory limit), with: a) the answer to their requests; b) a request for an additional month to comply with a suitable reason; or c) a refusal letter explaining why.

Data Protection Responsibilities

As part of our legal obligations for processing record keeping, it is critical that the Trust has complete control and awareness over the location and processing of all personal data. The Trust keeps an internal Data Processing Register, which records all data processing activities, the legal basis for processing, any associated third party processor and risk management provision.

It is the responsibility of Trust and all staff to ensure 'data protection by design' and 'data protection by default', by considering data protection in the development and operation of Trust activities.

Our responsibilities include:

- The Data Processing Register must be reviewed and updated every year by the DPO.
- Staff must consult the DPO before engaging in any new activity, which involves personal data.
- A data protection impact assessment (DPIA) query form (see **Appendix II**) must be completed by staff and submitted to the DPO for approval for any new activity processing personal data. A DPIA must be conducted and if approved, the results added to the Data Processing Register.
- Up to date malware and system monitoring tools must be used to assist in automatic detection of potential breaches.
- Information systems must be adequate and kept up to date.
- The DPO must liaise with the supervisory authority and notify relevant parties of any applicable data breaches.
- Documented staff training must be conducted annually and awareness maintained throughout the year.
- All new staff must complete recorded data protection training as part of their formal induction before being granted access to information systems.
- All staff leavers must return any personal data to the Trust (such as data in personal electronic markbooks/planners) as part of their formal exit process.
- Personal data must be disposed of properly. Physical copies must be shredded before disposal.

Subject Access Requests (SAR)
Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking.

A Subject Access Request can be made using the links below:

Regents Park:

https://app.jedu.tclhosting.co.uk/secure/information-request/$2y$10$bup2GwVyDC24RmIzwO4fGeUM9ilAZIO4N1FN46dBYX1cNnRhmu4n6

Sloane Square:

https://app.jedu.tclhosting.co.uk/secure/information-request/$2y$10$G2UtySD1EJ8zris7XG0khuqeNXs2y8NgW7x9oGu1VLoLp3IMEqwbu

DATA BREACH

Reporting a Data Breach

Any instances of data breach or suspected data breach must be reported immediately to the Director of Information Systems. The Information Commissioners Office (ICO) must be notified within 72 hours.

Procedure:

- Report the breach to The Director of Information Systems.
- Complete a data breach report form which will be sent once contact has been made the Director of Information Systems
- The detail in the form will be added to the breach log.

Where appropriate, those reporting the breach should liaise with their 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, Director of Information Systems or the Data Protection Officer.

Once reported, the reporter should not take any further action in relation to the breach. In particular they must not notify any affected individuals or regulators or investigate further. The Director of Information Systems 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, the Director of IT will notify the Data Protection Officer. 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 where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach; and
- Take steps to prevent future breaches.

Notifying the ICO

Judicium will notify the Information Commissioners Office (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, the most appropriate member of SLT will notify the affected individuals without undue delay including the name and contact details of the Data Protection Officer (DPO) and the 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, the Director of Information Systems 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 Director of Information Systems will 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. The Head and COO should be made aware of all data breaches and the chair of governors informed as necessary.

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 it is 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 and Cyber Security 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 do not meet the criteria of a data breach) that you may have to the Director of Information Systems 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.

Cyber security concerns should be reported to the Director of Information Systems and IT Support.

APPENDIX I
Francis Holland Schools Trust – Data Retention Schedule

The following table represents the periods for which specified information and data records must be retained.

The list is not exhaustive and where a particular retention guide does not exist, staff are expected to apply the best practice approach of retaining data for no longer than is necessary. Further guidance can be sought from the relevant senior member of staff or the Data Protection Officer.

Once a retention period has expired, the information/data must be erased.

Type of Record/Document	**Retention Period** [1]
Governance Records	
Registration documents of School	Permanent (or until closure of the school)
Attendance Register	6 years from last date of entry, then archive.
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
Pupil Records	
Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: - Pupil reports - Pupil performance records - Pupil medical records	ALL: 25 years from date of birth (subject where relevant to safeguarding considerations). Any material, which may be relevant to potential claims, should be kept for the lifetime of the pupil.
Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
Records of formal parental complaints under stage 2 or 3 of *Complaints From Parents Policy*	Minimum – 7 years
Centralised bullying records	For the duration of the pupil's time at the School, plus a maximum of 2 years.
Safeguarding	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]

Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low-level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).
Corporation Records	
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards, Governor or Management Meetings	Minimum – 10 years
Shareholder resolutions	Minimum – 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
Annual reports	Minimum – 6 years
Accounting Records [3]	
Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*)	Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
Contracts and Agreements	
Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
Intellectual Property Records	
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right, which can be permanently extended, e.g. trademarks); otherwise expiry of right plus minimum of 7 years.
Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement

Personnel Records	
Single Central Record of employees	Keep a record of all mandatory checks that have been undertaken (not certificate) until the next ISI inspection
Contracts of employment	7 years from effective date of end of contract
Employee appraisals or reviews	Duration of employment plus maximum of 7 years
Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
Payroll, salary, maternity pay records	Minimum – 6 years
Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	6 months
Immigration records	Minimum – 4 years
Health records relating to employees	7 years from end of contract of employment
Insurance Records	
Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
Correspondence related to claims/renewals/ notification re: insurance	Minimum – 7 years
Facilities and Health and Safety Records	
Maintenance logs	10 years from date of last entry
Accidents to children [4]	25 years from birth (unless safeguarding incident)
Accident at work records (staff) [4]	Minimum – 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances [4]	Minimum – 7 years from end of date of use
Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event or activity.

1. General basis of suggestions include mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011); practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO still expects to see a responsible assessment policy (e.g. every 6 years) in place.

3. Retention period for tax purposes driven by legal or accountancy guidelines.

4. Latent injuries can take years to manifest, and the limitation period for claims reflects this: a note should be kept of all procedures as they were at the time, with a record that they were followed. Relevant insurance documents should also be kept.

APPENDIX II

Francis Holland Schools Trust – Data Protection Impact Assessment (DPIA) Query Form

The live copy of this form is located in the virtual learning environment.

Staff Name:

Staff Job Title

Date:

Description of Activity
Purpose of the Activity
What personal data will be involved?
How long will the personal data to be kept?
What are the potential personal data risks?
How will personal data be protected?
Where will the data be stored (if online, which country)?