FHS
Francis Holland Schools

# Data Protection Policy

Table of Contents

# Data Protection Policy

**This policy applies to:**

**Francis Holland Regent's Park**
**Francis Holland Sloane Square**
**Francis Holland Prep**
**Francis Holland Schools Trust Business and Operations**

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

## Related Policies

Privacy Notices (see para 5)
Cybersecurity Policy

## 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 2021)*
- The Privacy and Electronic Communications Regulation 2011*
- *as amended by The Data Use and Access Act 2025
- The Protection of Freedoms Act 2012
- Joint Council for Qualifications – General Regulations for Approved Centres
- Data protection in schools (DfE guidance, updated 2024)

## 1. Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It 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.

Francis Holland Schools Trust, its Schools and staff, herein referred to as the **Trust**, are committed to treating the personal data of our pupils, parents, suppliers, employees, workers and other third parties in a responsible, open and trustworthy manner, which maintains compliance with data protection laws.

## 2. 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 2021) and the Data Protection Act 2018, both as amended by the Data Use and Access Act 2025. The Trust is registered with the Information Commissioners Office (ICO) as required Number Z1721394.

### 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 Processors are required to notify the School of any data breach without undue delay after becoming aware of the data breach (see paragraph 9). Failure to do so may result in a breach to the terms of the processing agreement between them and the Trust.

### Data Protection Officer (DPO)

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

Judicium Consulting Ltd
5th Floor,
98 Theobald's Road,
London WC1X
dataservices@judicium.com
0345 548 7000

## 3. 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.

## 4. 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.

## 5. 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. The Trust makes Privacy Notices available to the following stakeholders, and notifies them accordingly:

- Pupils and Parents
- Staff
- Job Applicants
- Governors and Volunteers
- Visitors and Contractors
- Alumni, Friends and Supporters

The Trust's Privacy Notices are available on the Trust website.

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

## 6. 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.

## 7. 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 (please see the Trust's Data Retention Policy). 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 Prep 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.

## 8. Sharing Data

FHST may need to share an individual's personal data with third parties, including third party service providers and other bodies where it is necessary to do so. There are strict controls on who can see your information. FHST will not share your data if you have advised us that you do not want it shared unless it's the only way FHST can make sure you stay safe and healthy, or FHST are legally required to do so.

When it comes to the Trust sharing information for safeguarding purposes with its safeguarding partners and other agencies (as it is required to do by law and statutory guidance), the following should be noted:

- Timely information sharing is essential to effective safeguarding;
- Fears about sharing safeguarding information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children;

- The Data Protection Act (DPA) 2018, UK GDPR 2021 and the Data Use and Access Act 2025 (DUAA) do not prevent, or limit, the sharing of information for the purposes of keeping children safe.

When the School is asked to share data with an organisation such as the police and other safeguarding agencies/partners, it does not need to decide whether that organisation needs the information to perform its public tasks or functions. Instead, the police or organisation making the request, is responsible for this decision.

## 9. 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.

## 10. 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 Director of Technology and/or Head of Compliance before engaging in any new processing activity, which involves personal data.
- A data protection impact assessment (DPIA) may then be completed by the Director of Technology and/or Head of Compliance for any such proposed new activity, if required.

Information to enable this assessment may be required from the staff members who have proposed it.

- The results of the DPIAs are logged by the Director of Technology.
- 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.
- All relevant personnel must undergo adequate training to enable them to comply with data privacy legislation. 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.

## 11. Subject Access Requests (SAR)

Under Data Protection Law, data subjects have a general right to find out whether the School holds or processes 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 is undertaking. All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

### 11.1 Time Period for Responding

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received. In both cases (proof of ID, and other clarification requested), the school will be unable to comply with the request if they do not receive the additional information.

The period for response to a SAR may be extended by a further two calendar months in relation to complex requests.

### 11.2 Validity of Requestor

A data subject is generally only entitled to access their own personal data and not information relating to other people, however an adult with parental responsibility may make a SAR regarding their child if they are under the age of twelve. A third party can also act on behalf of any individual provided they have the required authorisation.

It is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney.

For pupils aged twelve and over who are assessed by the school as mature enough to understand (in broad terms) what it means to make a subject access and interpret the information they receive as a result of doing so, then the school should usually respond directly to the child or seek their written authorisation before releasing their information.

### 11.3 Identity of Requestor

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees and current students, this will usually be straightforward. In other cases, evidence of identity may be established by production of a passport, driving licence, a recent utility bill with current address, birth/marriage certificate, or a mortgage statement. When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

### 11.4 Complex Requests

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

### 11.5 A 'Reasonable and Proportionate' Data Search

The UK GDPR underlines that organisations only have to undertake 'reasonable and proportionate' searches for a person's personal information. A guide to subject access | ICO

### 11.6 Exemptions from Providing Certain Information

The DPA sets out certain exemptions to the obligations to give access to data under an SAR. For example, the School may withhold some of the information for safeguarding purposes, specifically because the information might cause serious harm to the physical or mental health of the pupil or another individual, or it would not be in the best interests of the child (data subject) itself.

The school also does not have to disclose any confidential references given to, or received from, third parties for the purpose of education, training or employment, nor any personal data being processed for the purposes of preventing or detecting crime.

This is not an exhaustive list, full details can be found at What other exemptions are there? | ICO

### 11.7 School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because, depending on the nature of the data requested, the appropriate staff needed to comply with the request may not be available during this time.

We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request), but the School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is

urgent, please provide your request during term times and not during/close to closure periods.

### 11.8 Refusing to Respond to a Request

There are certain occasions where the school can refuse to comply with a request, for example where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. For a list of other such occasions, please see When can we refuse to comply with a request? | ICO

If that is the case, the data subject will be informed by the School, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy

### 11.9 How to Make a Subject Access Request

A Subject Access Request can be made using the links below, however it will be equally valid if made directly to the School:

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

Prep:
https://www.jedu.co.uk/secure/information-request/$2y$10$TOyDlCubtTduyzzXx8hi9uidLv8bse0CfIVMP7ArCMw7bxQnZltmy

### 11.10 Record Keeping

A record of all subject access requests shall be kept by the Trust. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

## 12. Data Breaches

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. A breach can happen when data is being processed at the Trust, or at one of the Third-Party Processors that have been contracted to process personal data on the Trust's behalf.

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.

Under the UK GDPR, it is important to distinguish the responsibilities of Data Controllers and Data Processors in the event of a personal data breach:

- Data Controller
  The Trust acts as the Data Controller, meaning it determines the purposes and means of processing personal data. The Data Controller has the primary responsibility for ensuring compliance with UK GDPR, including reporting data breaches to the ICO (Information Commissioner's Office) within 72 hours when required, and communicating with affected individuals if there is a high risk to their rights and freedoms. The Data Controller must also keep records of all breaches and take appropriate steps to contain and mitigate the impact of any breach.

- Data Processor
  Data Processors are external organisations or individuals who process personal data on behalf of the Data Controller (e.g., third-party service providers). Processors must implement appropriate technical and organisational measures to protect personal data and notify the Data Controller without undue delay upon becoming aware of any personal data breach.

  Data Processors are 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.

For full details regarding how the Trust handles data breaches, staff refer to the Trust's Data Breach Guidance and Procedure document.

## 13. 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 Technology 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 immediately to the Director of Technology and IT Support.

## 14. Breaches of this Policy

All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Staff is defined as employees, governors, trustees and volunteers. Breaches 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 dismissal depending on the seriousness of the breach.

## 15. Audit

The Trust, through its Data Protection Officer, regularly tests its data systems and processes in order to assess compliance via annual data audits to review its use of personal data.

## 16. Changes to this Policy

We reserve the right to update this Data Protection Policy at any time, and we will provide you with a new Policy when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

## 17. Complaints about our Handling of Personal Data

Data protection legislation requires organisations to help any person who wants to make complaints about how their personal information is used. The Trust therefore has an electronic complaints form (here) on which people may submit details to us regarding their complaint. This complaint form will be acknowledged within 30 days and responded to without undue delay.

We have appointed a Data Protection Officer (DPO) to oversee compliance with data protection and this privacy notice. You may also, if you wish, contact them:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobald's Road, London WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk

## 18. Review

| | |
|---|---|
| Policy author/s | Trust: Director of Technology |
| This review | Spring 2026 |
| Approved by | SLTs: Spring 2026<br>Governance and Nominations: Spring 2026 |
| This version published | June 2026 |
| Next review | Spring Summer 2027 |

The Francis Holland Schools Trust is an educational charity which manages three leading independent girls' schools in central London, across three sites.
Registered charity number: 312745
Registered office: Francis Holland Schools Trust, 35 Bourne Street, London SW1W 8JA