FRANCIS HOLLAND
SCHOOLS TRUST

Data Protection Policy

Francis Holland Schools Trust
April 2018

1. Introduction

1.1 This statement is aimed at all pupils, including those in the EYFS, parents and alumnae and explains how Francis Holland Schools Trust (the Trust) uses personal information.

1.2 The Trust, its Schools and staff are committed to treating personal data in a responsible, open and trustworthy manner, which maintains compliance with data protection laws.

1.3 The Trust's use of personal information is covered by the following legal and regulatory mechanisms:

- The Data Protection Act 1998
- The General Data Protection Regulation (GDPR) 2016
- The Privacy and Electronic Communications Regulation 2011
- The Protection of Freedoms Act 2012
- Joint Council for Qualifications – General Regulations for Approved Centres

The purpose of these laws/regulations is to safeguard personal information. They cover issues such as data security, individuals' rights to access information about themselves and the use and disclosure of personal information.

2. Terminology

2.1 **Personal Data** – any data relating to a living individual (i.e. staff, pupils, parents/guardians and third parties). **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. Both personal data and Special Categories of personal data (Sensitive personal data) will be referred to as **personal data** in this policy.

2.2 **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. The Trust is the Data Controller under the General Data Protection Regulation 2016 and the Data Protection Act 1998/2018.

2.3 **Data Processor** – does something with the data, including recording, collecting, storing and analysing. The Trust is a Data Processor under the General Data Protection Regulation 2016 and the Data Protection Act 1998/2018. 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.

2.4 **Breach** – defines anything leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.5 **Data Protection Co-ordinator (DPC)** – the Trust's primary point of contact for data protection duties. The DPC liaises with the Information Commissioner's Office (ICO), monitoring and reporting on compliance. The Director of Information Systems is the Trust's DPC and can be contacted as follows:

Email: dpc@fhst.org.uk

Data Protection Coordinator (DPC)
Francis Holland Schools Trust
35 Bourne Street
London SW1W 8JA

3. How the Trust acquires personal data

3.1 The Trust may acquire such personal data in a number of ways. For example:

- parents or pupils may provide the Trust with personal data about themselves or their family in correspondence, forms, documents, during discussions with staff, and through Trust websites;
- the Trust may acquire personal data from other parents or pupils, or from people outside of the Trust community who know parents or pupils of the Trust;
- the Trust may acquire personal data from other Trusts, public authorities, public sources or from commercial sources such as credit reference agencies; and
- the Trust may acquire personal data through the recording of still and video images from CCTV and other sources.

4. How the Trust uses personal data

4.1 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

4.2 The Trust commonly uses such personal data for:

- ensuring that the Trust and its Schools are a safe and secure environment;
- providing education and pastoral care;
- providing academic, examination and career references for pupils;
- providing additional activities for pupils and parents - this includes school trips and activity clubs;

- protecting and promoting the interests and objectives of the Trust - this includes fundraising and alumnae relations;
- safeguarding and promoting the welfare of pupils; and
- fulfilling the Trust's contractual and other legal obligations.

4.3 The Trust, as a Controller, is responsible for, and must be able to demonstrate, compliance with the following 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.

4.4 The Trust will not use pupil / parent personal data for direct marketing purposes if you ask us not to.

Disclosure Exemptions

4.5 The Trust may use personal data for other purposes where the law allows and where providing an explanation would not be appropriate. This includes:

- Data subject consent.
- National security interests.
- In the prevention and investigation of crime and prosecution of offenders.
- To prevent serious harm.
- Legal and regulatory obligations.
- In connection with legal proceedings or advice.

4.6 The Trust will not use personal data for any other purpose unless it has first communicated the other purposes to pupils or parents, or the DPC considers it is reasonable and fair to do so.

Third Parties and Cloud Providers

4.7 The Trust does not share personal data with third parties unless it is fair to do so.

4.8 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, catering, development initiatives and communications.

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

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

4.11 The Trust must not process or use any third party processor involving transferring personal data outside the European Economic Area (EEA).

5. Data processing guidelines

5.1 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 DPC.

The core processing rules that all staff must follow to ensure adequate levels of data protection are:

- 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 version must be deleted and physical copies destroyed and disposed.
- 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.
- Emails will have a retention period of six months before auto deletion, unless flagged for retention.
- 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 platform must be used, unless otherwise approved by the DPC.
- Cloud services must be approved by the DPC 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 DPC 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 remote access should be used instead. Where unavoidable, encrypted USB storage must be used.
- All school mobile devices must have encryption enabled.
- Staff must use remote access platforms if working with data offsite. Where unavoidable, limited personal data can be processed by staff on personal devices in support of school work. 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.

6. Data subject statutory rights

6.1 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 DPC within one working day.
- The DPC 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 DPC 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.

6.2 **Subject Access Request:** Subject to a number of exemptions contained in the Act, parents and pupils have a statutory right to know if the Trust holds any personal data about them, and to know what it is, its source, how the Trust uses it, the logic the Trust uses in any automatic decisions, and who the Trust discloses it to. Parents or pupils who wish to access this information will need to make a Subject Access Request. This can be done by submitting a request **in writing** and paying the appropriate fee (usually £10). The Trust will respond to a request within 40 days from when it receives the request in writing, any further information reasonably requested by the Trust and (if the Trust asks for it) the fee.

6.3 **Automatic decisions**: Parents and pupils have a statutory right to ask the Trust not to make decisions automatically (using personal data) if such automatic decisions would affect them to a significant degree.

6.4 **Corrections:** Parents and pupils have a statutory right to ask for incorrect personal data to be corrected or annotated.

6.5 **Use of personal data:** Parents and pupils have a statutory right to ask the Trust not to use their personal data in a way that is likely to cause them unwarranted and substantial damage or distress.

7. Data protection responsibilities

7.1 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.

7.2 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 DPC.
- Staff must consult the DPC 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 DPC 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 DPC 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.

8. Further Information

8.1 The purpose of this statement is to explain how the Trust uses personal data about pupils and parents. It does not, and is not intended to, place any obligation on the Trust greater than that set out under the GDPR.

8.2 **ICO website:** Further details of the personal data the Trust holds, and how the Trust uses it, can be found in the Trust's register entry on the Information Commissioner's website at www.ico.org.uk under registration number **CSN2173419**. This website also contains further information about data protection.

8.3 **Contact:** If you would like any further information about anything within this statement then please contact the DPC.

9. Review

9.1 This policy will be reviewed by the DPC on each anniversary of the effective date of the policy and immediately following any data protection related incident.

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.
Minutes of Governors' meetings	6 years from date of meeting
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)
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 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. trade marks); 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 permanent record of all mandatory checks that have been undertaken (not certificate)
Contracts of employment	7 years from effective date of end of contract

Employee appraisals or reviews	Duration of employment plus minimum 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)	Minimum 3 months but no more than 1 year
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)?