DATA PROTECTION POLICY

Introduction

In order to carry out their statutory, academic and administrative functions, the Leys School and St Faith's School (part of The Leys and St Faith's Schools Foundation and together referred to in this policy as the "Schools") must collect and process Personal Data (as defined below) relating to their staff, pupils and their parents and/or guardians, suppliers/contractors, visitors and other third parties with whom they deal.

The Schools take the confidentiality of all Personal Data very seriously and take all reasonable steps to comply with the principles of the United Kingdom General Data Protection Regulation and Data Protection Act 2018.

It is the Schools' objective only to collect Personal Data to meet specifically planned, agreed and necessary purposes, and to retain that information no longer than is necessary. This Data Protection Policy (the "Policy") sets out the overall principles that will apply to the Processing of Personal Data and Special Category Data at the Schools.

Definitions

For the purposes of this Policy:

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

"Data Controller" means a person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be processed. The Schools are Data Controllers.

"Data Processor" means any person (other than an employee of the data controller) or organisation who processes data on behalf of the Data Controller.

"Data Protection Legislation" means (i) the United Kingdom General Data Protection Regulation ("GDPR") and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the United Kingdom and (ii) any successor legislation to the GDPR.

"Data Subject" for the purposes of this Policy includes all living individuals about whom the Schools hold Personal Data. A Data Subject need not be a UK national or resident.

"Data Subject Access Request" means an individual's exercise of their right of access, which gives them the right to obtain a copy of their Personal Data.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"Processing" or **"Processed"** or **"Processes"** means any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Special Category Data" includes details about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Protection Principles
The Schools process Personal Data in accordance with the following data protection principles listed in Data Protection Legislation:

- Personal Data is processed fairly, lawfully and transparently;
- Personal Data is collected for specified, explicit and legitimate purposes and data is not then processed in a manner which is incompatible with those purposes;
- Personal Data processed is adequate, relevant and limited to what is necessary;
- Personal Data is kept accurate and the Schools take reasonable steps to ensure that inaccurate Personal Data is rectified or deleted without delay;
- Personal Data is not kept for longer than is necessary;
- The Schools adopt measures to keep Personal Data secure when processed and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Schools inform individuals of the reasons for processing their Personal Data, how they use such data and the legal basis for processing the data in their Privacy Notices. Copies of the Schools' Privacy Notices can be found on their respective websites or on request.

Where the Schools process Special Category Data, this is also done in accordance with Data Protection Legislation.

Data Protection Responsibilities

1. Data Controller Responsibilities
The Schools are Data Controllers under Data Protection Legislation, and the Governors have overall responsibility for monitoring this Policy and ensuring that it is implemented.

The Schools will apply strict safeguards to the Processing of Personal Data and Special Category Data and will manage that data appropriately to abide by the six data protection principles.

The Schools as Data Controllers will take all reasonable measures to ensure:

- Personal Data and Special Category Data is Processed, collected, held, transferred and disposed of in a fair, lawful and secure way
- Anyone who wants to exercise their right of access to their Personal Data is made aware of the process and requests are handled courteously, no matter the outcome
- Data Subject Access Requests, once received, are dealt with promptly and efficiently
- Staff members are made aware of and understand their duties under Data Protection Legislation/guidance and the respective School's policies and procedures
- There is an individual at each School who has specific responsibility for data protection matters
- Methods of Processing Personal Data and Special Category Data are reviewed in accordance with any changes in Data Protection Legislation or guidance
- GDPR requirements will feature throughout the Schools' decision-making processes and especially in the development of any policy, design or implementation of IT systems and/or the monitoring or evaluation of those systems and their performance

The above list is not exhaustive but is meant as a guide as to the types of steps the Schools take to comply with Data Protection Legislation.

2. Staff Responsibilities

All staff members have a duty to assist the Data Controller with data protection compliance, including complying with the data protection principles and this Policy at all times. Any breach of these may result in disciplinary action.

When staff, as part of their duties, collect information about other people (e.g. about students' coursework, opinions as to ability, references from other academic institutions, or details of personal circumstances), they must comply with the following requirements:

- Any Personal Data which staff hold must be kept securely (e.g. in a locked environment, encrypted or password protected if it is electronic). Where staff remove hard copy Personal Data from the school site (such as pupil workbooks), this must be held securely and not left unattended in public places;
- Staff must only access Personal Data they have authority to access it and only for authorised purposes;
- Personal Data is not disclosed orally, in writing or by any other means, either accidentally or otherwise to any unauthorised third party. This includes for example, sending e-mails to the wrong recipient.

3. Data Subject Responsibilities

All Data Subjects (e.g. staff, pupils, parents, alumni) are responsible for:

- Checking that all the information they provide to the respective School is accurate and up to date;

- Promptly informing the respective School of any changes to their Personal Data;
- Checking Personal Data sent out from the respective School from time to time;
- Informing the respective School of any errors or changes. The Schools cannot be held responsible for any errors unless the Data Subject concerned has informed the relevant School of them.

4. Data Processor Responsibilities

All Data Processors that the Schools use also have responsibilities under Data Protection Legislation. These include (but are not limited to):

- Cooperating in terms of having a written Data Processing Agreement in place with the Schools;
- Processing Personal Data on behalf of the Schools in accordance with Data Protection Legislation and only for the provision of the agreed services to the Schools;
- Ensure that their employees, agents and any sub-processors are made aware of and trained in their responsibilities under Data Protection Legislation;
- Assist as far as reasonably possible with Data Subject Access Requests and Data Breaches made in connection with the services to the Schools.

Data Subject Rights

Data Protection Legislation provides the following rights for individuals which can be exercised in certain circumstances:

- The right to be informed. The Schools provide information on how Personal Data is processed (detailed in the respective Privacy Notices);
- The right of access. This allows individuals the right to access their Personal Data and supplementary information;
- The right to rectification. This gives individuals the right to have Personal Data rectified if inaccurate or incomplete;
- The right to erasure. This enables an individual to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing;
- The right to restrict processing. Individuals have a right to 'block' or suppress processing of Personal Data;
- The right to data portability. Allows individuals to obtain and reuse their Personal Data for their own purposes across different services;
- The right to object. Individuals have the right to object to the processing of Personal Data, for example where Personal Data are processed for direct marketing purposes;
- Rights in relation to automated decision making and profiling. Additional rules have been introduced to protect individuals where automated decision-making is being carried out. This includes introducing ways for individuals to request human intervention and challenge decision making and ensuring organisations carry out regular checks to ensure systems are working as intended.

In order to rectify parent or pupil data, requests should generally be submitted to the School Office of the appropriate School. To rectify staff data, requests can be made to the Human Resources department of the appropriate School.

All other requests should be sent to the Data Compliance Officers at the appropriate School:

- St Faith's: by email at gdpr@stfaiths.co.uk, or in writing to St Faith's School, Trumpington Road, Cambridge, CB2 8AG.
- The Leys: by email at compliance@theleys.net, or in writing to The Leys School, Trumpington Road, Cambridge, CB2 7AD.

Right to Access Personal Data

Data Subjects have the right under the UK GDPR to obtain confirmation as to whether or not their Personal Data is being Processed by either School and to access that Personal Data. To exercise this right, they must make a Data Subject Access Request (DSAR). This can be done by contacting in writing the Data Compliance Officer at the respective School (see details above).

In most cases the Schools will need to ask for proof of identification before a request can be processed. The relevant School will inform the individual if it needs to verify their identity and the documents it requires.

DSARs will be dealt with as quickly as possible and certainly within the stipulated one month from receipt of the request. For complex or numerous DSARs then the School may extend the period by a further two months. If this is the case then the individual concerned will be notified within one month of receipt of the request with an explanation as to why the extension is necessary.

If a DSAR is manifestly unfounded or excessive, the School may refuse to action the request. Alternatively, the School can agree to respond but charge a fee, which will be based on the administrative cost of responding to the request. A DSAR is likely to be manifestly unfounded or excessive, for example, where it repeats a request to which the School has already responded. If an individual submits a request that is unfounded or excessive, the School will notify them that this is the case and whether or not it will respond.

Requests that Cannot be Fulfilled

Individuals should be aware that the right of access is limited to their own Personal Data and certain data is exempt from the right of access. This may include information which identifies other individuals or information which is subject to legal privilege (for example legal advice given to or sought by the Schools, or documents prepared in connection with a legal action).

The right to erasure is limited as the Schools will often have compelling reasons to refuse specific requests to delete data. For example, in order to comply with a legal or safeguarding requirement, or where there are overriding legitimate grounds. All such requests will be considered on their own merits.

Children's Rights over their Personal Data

The rights under the UK GDPR are the individuals to whom the Personal Data relates. However, the law recognises children's rights to have a say over how their Personal Data is used from the age of 13. Therefore, St Faith's will in the majority of cases rely on parental consent to Process Personal Data relating to pupils unless, given the nature of the Processing in question and the pupil's age and understanding, it is unreasonable in all the circumstances to rely on the parent's consent. Parents should be aware that in such situations they may not be consulted. At The Leys, the School will

generally only rely on parental consent for under 13-year-old pupils and rely on pupils' consent if they are over the age of 13.

If a young person is deemed incapable of making their own decisions, the primary parent/carer/guardian will act on their behalf. This authority is only extended to functions that are in the best interests of the child.

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds agreement to Personal Data being disclosed to a parent or guardian, the relevant School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils.

Where opinions regarding the use of a pupil's Personal Data conflict between the pupil and their parent, the Schools will make every effort to reach a solution in which both parties are comfortable.

Data Security

Please refer to the Information Security Policy.

Disclosure of Personal Data

The Schools may receive requests from third parties to disclose personal data. The Schools will not generally disclose information unless the individual has given their consent or it is to be disclosed for a legitimate business interest, such as:

- Giving a pupil reference to an educational institution that the pupil may attend;
- Giving information relating to outstanding fees or payment history to an educational institution which a pupil may attend;
- Disclosing details of a pupil's public examinations or other achievements of pupils at the Schools;
- Disclosing details of a pupil's medical condition where it is in the vital interests of the pupil to do so.

Where the Schools receive a disclosure request from a third party they will take reasonable steps to make the disclosure secure, such as verifying the identity of the third party, putting data protection agreements in place and analysing privacy notices where relevant.

International Data Transfer

All pupils, staff members and other individuals who handle School Data must not transfer Personal Data outside the UK without first consulting the relevant Data Compliance Officer. The Schools have a duty to put adequate safeguards in place (where reasonably possible) so that the Personal Data would be protected in such a transfer.

Data Retention

The periods for which the Schools normally retain Personal Data are contained within their respective Retention Policies, which are based on the Information Management Toolkit for Schools (Information and Records Management Society).

Data Breaches

In the event of a breach both Schools will follow the procedures in their respective Data Security Breach Management Policies.

Data Protection Registration

As the Schools are considered Data Controllers, they are required by the Information Commissioner's Office to be registered on their Data Protection Public Register (https://ico.org.uk/esdwebpages/search). The Information Commissioner's Office acts as the UK regulator for data protection purposes. The Schools are registered under The Leys and St Faith's Schools under registration number Z570129X.

Queries/Complaints

The Schools aim to handle any queries, concerns or complaints relating to the Processing of Personal Data promptly and courteously. These should be raised in the first instance with the relevant Data Compliance Officer, details of which are given above. The Data Compliance Officer will decide whether it is appropriate to follow the School's Complaints Procedure (please see the Schools' Complaints Policies for more information, available on their respective websites.)

If you would like to take the matter further you may contact the Information Commissioner's Office (ICO) by contacting 0303 123 1113. More information on complaints to the ICO is available here https://ico.org.uk/make-a-complaint/.

Policy Review

This Policy will be amended from time to term and no less than annually. Any changes we make will be posted on the Schools' respective websites and where appropriate, notified to Data Subjects.

Related Policies

Policies related to this Data Protection Policy (where applicable) are:

- Information Security Policy
- Respective Privacy Notices
- Data Retention Policy
- Acceptable Use Policy
- Network and Social Media Acceptable Use Policy
- Remote Working Policy
- Data Security Breach Management Policy