DATA PROTECTION POLICY

INTRODUCTION

In order to carry out its statutory, academic and administrative functions, St Faith's must collect and process personal data (as defined below) relating to its staff, pupils and their parents and/or guardians, suppliers, contractors and other individuals with whom it deals. The School takes the confidentiality of all personal data very seriously and takes all reasonable steps to comply with the principles of the General Data Protection Regulation. It is the School's objective only to collect personal data necessary to meet specifically planned, agreed and necessary purposes, and to retain that information no longer than is necessary.

The Governors have the ultimate authority for Data Protection within the School, but the Operations Manager has been designated as the Data Compliance Officer and is responsible for the day-to-day management of Data Protection within the School.

The Data Compliance Officer can be contacted by email at GDPR@stfaiths.co.uk or by phone on 01223 229443.

Full details of the School's registration under current Data Protection legislation can be found on the Data Protection Register website (www.ico.org.uk) under the registration number Z976867X.

DEFINITIONS

Data Protection Legislation: means (i) the General Data Protection Regulation (EU) 2016/679 ("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.

Personal Data: Any information that relates to an individual who can be identified from that information, whether directly or indirectly.

Processing: Any operation performed on personal data, including collecting, using, storing, amending, disclosing or destroying it.

Special categories of personal data: Means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health (both physical and mental), sex life or sexual orientation and biometric data.

Criminal records data: Means information about an individual's criminal convictions and offences, and information relation to criminal allegations and proceedings.

Staff: Includes any individual who might apply to work, does work or has worked for St Faith's School, and/or any of its associated organisations (e.g. St Faith's Parent Association or the Old Fidelian Society) and individuals who come to the School on work experience placements or volunteers.

Pupils: Includes prospective, current and past pupils.

DATA PROTECTION PRINCIPLES

The School processes personal data in accordance with the following data protection principles:

- The School processes personal data lawfully, fairly and in a transparent manner;
- The School collects personal data only for specified, explicit and legitimate purposes, and data is not then processed in a manner which is incompatible with those purposes;
- Personal data processed by the School is adequate, relevant and limited to what is necessary for the purposes of processing;
- Personal data kept by the School is accurate, and the School takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- The School keeps personal data for no longer than is necessary;
- The School adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The School informs individuals of the reasons for processing their personal data, how it uses such data and the legal basis for processing the data in its privacy notices. A copy of the School's privacy notices are available on the School's website and virtual learning environment (VLE).

The School will not process personal data of individuals for other reasons not set out in this policy or the privacy notices.

Where the School processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the Data Protection Legislation.

RETENTION OF DATA

The periods for which the School holds personal data are contained in its Data Retention Policy.

This retention schedule is based on guidance from the Information and Records Management Society: http/www.irms.org.uk

The School toolkit encompasses records managed by all types of schools – some of the file descriptions listed may not be relevant to every school.

DISCLOSURE OF PERSONAL DATA

The School may receive requests from third parties to disclose personal data it holds about staff, pupils, their parents or guardians. The School confirms that it will not generally disclose information unless the individual has given their consent or it is to be disclosed for a legitimate business interest

The School does intend to disclose such personal data as is necessary to third parties for the following purposes:

- To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend.
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend.
- To publish the results of public examinations or other achievements of pupils of the School.
- To disclose details of a pupil's medical condition where it is in the pupil's vital interest to do so. To meet the legal obligations of the Data Controller in relation to the ContactPoint national database which is planned to contain limited information about every child in England.

Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

INTERNATIONAL DATA TRANSFER

All staff must not transfer Personal Data outside the European Economic Area and/or internationally without first consulting the Data Compliance Officer.

The School has a duty to first ensure that adequate safeguards are in place so that the Personal Data would be protected in such a transfer, if that transfer was considered appropriate.

RIGHTS AND RESPONSIBILITES

INDIVIDUAL RIGHTS

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

- The right to be informed. Organisations must provide information on how Personal Data is processed (this will normally be detailed in an organisations privacy notice);
- 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 where this has been done for the purposes of a legitimate interest or for the performance of a task in the public interest/exercise of official, for direct marketing purposes or for the purposes of scientific/historical research and statistics;
- 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 data, requests should be submitted to either the School Office (pupil/parent/carer/guardian data) or the Human Resources and Safeguarding Co-ordinator (staff data).

To ask the School to take any of the other above steps, the individual should send a request to the Data Compliance Officer.

RIGHTS TO ACCESS INFORMATION

Pupils and their parents, staff of the School and other individuals have the right to obtain confirmation as to whether or not their Personal Data is being processed by the School and access to that Personal Data. To access their data they must make a Subject Access Request (SAR). Any person who wishes to exercise this right should apply to the Data Compliance Officer by completing the necessary form or submitting a written request.

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

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

If a SAR is manifestly unfounded or excessive, the School may refuse to act on the request. Alternatively, the School can agree to respond but will charge a fee, which will be based on the administrative cost or responding to the request. A SAR is likely to be manifestly unfounded or excessive 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 is the case and whether or not it will respond.

REQUESTS THAT CANNOT BE FULFILLED

You should be aware that the right of access is limited to your 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 School, or documents prepared in connection with a legal action).

You may have heard of the "right to be forgotten". However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your personal data: for example, in order to comply with a legal requirement, or where there are overriding legitimate grounds. All such requests will be considered on their own merits.

ACCESS TO PUPIL RECORDS

The rights under the Data Protection Legislation belong to the individual to whom the data relates.

The School will however in most 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. As a general rule children aged 13 and over may be expected to make reliable decisions regarding their personal information but the School will only grant the pupil direct access to personal data if in the School's reasonable belief the pupil understands the nature of the request.

If a young person is deemed incapable of making their own decisions, which is generally accepted as under the age of 13, the primary carer or guardian will act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or person.

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 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 of other pupils.

INDIDVIDUAL RESPONSIBILITIES

All individuals (e.g. staff, students and pupils and their parents) are responsible for:

- Checking that all information they provide to the School in connection with their employment or course of study is accurate and up to date;
- Promptly informing the School of any changes to their Personal Data;
- Checking Personal Data sent out by the School from time to time;

- Informing the School of any errors or changes. The School cannot be held responsible for any errors unless the individual concerned has informed the School of them.

If anyone on whom the School holds information believes that this policy has not been followed in respect of personal data about themselves, they should raise the matter initially with the Data Compliance Officer.

If the matter is not resolved it may be taken further by following the School Grievance Procedure or the School Parental Concerns and Complaints Policy. Similarly, if anyone believes that the correct policies are not being followed with regard to another individual's personal information, the facts should be reported to the Data Compliance Officer.

STAFF RESPONSBILITIES

All School staff who process or use any personal information must ensure that they follow the current Data Protection Principles at all times and follow the guidance and instructions contained in this policy. Any breach of these Principles or of the School's Data Protection Policy can have very serious and harmful consequences.

Accordingly, while this policy does not form part of the formal contract of employment, it is a condition of employment that staff shall adhere to the Principles and abide by the requirements of this policy.

If and when, as part of their duties, staff collect information about other people, (e.g. about students' course work, 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 (in a secure environment or password protected if is computerised).
- Staff must only access Personal Data they have authority to access it and only for authorised purposes.
- Personal information is not disclosed orally, in writing or by any other means, either accidentally or otherwise to any unauthorised third party. This includes, for example, home telephone numbers.
- Staff must not remove personal data, or devices containing or that can be used to access personal data, from the School's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

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

Any breach of this policy may lead to disciplinary action and in serious cases may be regarded as gross misconduct.

DATA SECURITY

The School takes the security of Personal Data seriously. The School has internal policies and controls in place to protect Personal Data against loss, accidental destruction, misuse or disclosure, and to ensure that Personal Data is not accessed, except by staff in the proper performance of their duties.

Policies which relate to data security include the School's CCTV policy and network and social media policy.

Where the School engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

DATA BREACHES

If the School discovers that there has been a breach of security in relation to Personal Data that is likely to pose a risk to the rights and freedoms of individuals, it will report the breach to the Information Commissioner's Office (ICO) within 72 hours of discovery. The School will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures the School has taken.

CHANGES TO THIS POLICY

We may update this policy at any time. Any changes we make to this privacy policy in the future will be [posted on the Schools website and VLE and, where appropriate, notified to you by e-mail.

RELATED POLICIES

St Faith's adopts the following policies that relate to the Data Protection Policy:

- CCTV Policy
- Network and Social Media Acceptable Use Policy
- Data Retention Policy
- Remote Working Policy
- Recruitment and Selection Policy
- Respective Privacy Notices

N L HELLIWELL
Headmaster