Data Protection Policy

Contents

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 ("Parent(s)"), 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.

This Policy does not form part of any individual terms and conditions of employment with the Schools and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Section 1 - 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 ("UK 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 UK 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.
Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data may be stored electronically or in hard copy.

"Processing" or **"Processed"** or **"Processes"** means any operation or set of operations which is performed on Personal Data or on sets of personal data, 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.

"Automated Processing" means any form of automated processing of personal data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning, but not limited to, staff members performance at work, the economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Special Category Data" includes details about a person's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data, and personal data relating to criminal offences and convictions.

Section 2 - When can the Schools Process Personal Data?

Data Protection Principles

The Schools are responsible for and adhere to the principles relating to the processing of Personal Data as set out in the UK GDPR. The principles the School must adhere to are set out below:

- *Personal Data is processed fairly, lawfully and transparently*

  The Schools only collect, process and share Personal Data fairly and lawfully and for specified purposes. The Schools must have a specified purpose for processing Personal Data and Special Category Data as set out in the UK GDPR.

  Before processing starts for the first time, the Schools will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. The Schools will review those purposes whilst processing of Personal Data continues in order to ensure that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data Processing Conditions	Special Category Data Processing Conditions
The Data Subject has given their consent	The Data Subject has given their explicit consent
The processing is necessary for the performance of a contract with the Data Subject or for taking steps at their request to enter into a contract	The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Schools in the field of employment law, social security law or social protection law
To protect the Data Subject's vital interests	To protect the Data Subject's vital interests
To ensure the School's comply with laws and regulations (other than contractual obligations)	The processing is necessary for the establishment, exercise or defence or legal claims or whenever courts are acting in their judicial capacity
To perform a task in the public interest or in order to carry out official functions as authorised by law	To perform a task in the substantial public interest or in order to carry out official functions as authorised by law
For the purposes of the Schools' legitimate interests where authorised and in accordance with, data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the Data Subject.	Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of employees, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
	Where it is necessary for reasons of public interest in the area of public health
	The processing is necessary for archiving, statistical or research purposes
	Where the data has been made public by the Data Subject

The School identifies and documents the legal grounds being relied upon for each processing activity.

- *Consent:*

  Where the Schools rely on consent as a fair condition for processing (as set out above), they will adhere to the requirements set out in the UK GDPR.

  Consent must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they signify agreement to the processing of Personal Data relating to them.

  A Data Subject will have consented to processing of their non-special category Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

  Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

  In cases of processing Special Category Data and explicit consent, the Schools will normally seek another legal basis to process that data. However, if explicit consent is required, the Data Subject will be provided with full information in order to provide explicit consent.

- *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:*

  The Schools will not use Personal Data for new, different or incompatible purposes from that disclosed, when it was first obtained, unless we have informed the Data Subject of the new purpose (and they have consented, where necessary).

- *Personal Data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed:*

  The Schools will only process Personal Data when our obligations and duties require us to do so. The Schools will not collect excessive data and will ensure any personal data collected is adequate and relevant for the intended purposes.

  When Personal Data is no longer required for specified purposes, the Schools shall delete or anonymise the data. Please refer to the individual Schools' Data Retention Guidelines/Policy for further guidance.

- *Personal Data is kept up to date and where necessary, the Schools take reasonable steps to ensure that inaccurate Personal Data is rectified or deleted without delay:*

  The Schools will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the Personal Data at the point of collection and reviewing the data collected, as and when necessary. The Schools will take reasonable steps to destroy or amend inaccurate or out of date Personal Data.

  Data Subjects also have an obligation to inform the School of any changes to their Personal Data to ensure that their data is accurate, complete, up to date and relevant.

- *Personal Data is not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed:*

  The Schools will take reasonable steps to destroy or erase all Personal Data from our current systems that we no longer require. We will also ensure that Data Subjects are informed of the period for which Personal Data is stored and how that period is determined in our privacy notices.

  Please refer to the Schools' Retention Guidelines/Policy for further details about how the Schools' retain and destroy data.

- *The Schools adopt measures to keep Personal Data secure when processed and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage:*

  In order to ensure the protection of all data being processed, the Schools will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:
  - Encryption;
  - Pseudonymisation (this is where the Schools replace information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
  - Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the Personal Data are authorised to access it);
  - Adhering to confidentiality principles;
  - Ensuring Personal Data is accurate and suitable for the purpose for which it is processed.

The Schools follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing Personal Data.

The Schools will only transfer Personal Data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the School's security measures are set out in the School's Information Security Policy. 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.

Sharing Personal Data

The Schools will generally not share Personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the Personal Data complies with the privacy notice that has been provided to the Data Subject and, if required, the Data Subject's consent has been obtained or there is another legal basis on which to share the Personal Data;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the Schools are required either by law or in the best interests of our pupils, Parents or staff to pass information onto external authorities for example, the police, the Local Authority, the Independent Schools Inspectorate (ISI) or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The School will take reasonable steps to make the disclosure secure, including verifying the identity of the third party.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The Schools will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Schools' guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The Schools may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

Section 3 – Data Subject's Rights and Requests

Data Subject Rights

Personal Data must be made available to Data Subjects as set out within this policy and Data Subjects must be allowed to exercise certain rights in relation to their Personal Data. 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 by submitting a Data Subject Access Request (DSAR). Further information can be found in Appendix 1 of this Policy;
- **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.
- **The right to withdraw consent**. This can occur at any time during the duration of processing, where consent is relied upon as a condition of processing.

Additional Data Subject Rights include, but are not limited to:

- Challenge processing which has been justified on the basis of the Schools legitimate interest or in the public interest;
- Request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- Object to decisions based solely on automated processing;
- Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales (ICO), https://ico.org.uk/global/contact-us; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structed, commonly used and machine-readable format.

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

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.

Direct Marketing

The Schools are subject to certain rules and privacy laws when marketing. For example, a Data Subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Schools will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Schools will promptly respond to any individual objection to direct marketing.

Section 4 - Data Protection Responsibilities and Accountability

The Schools will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. The Schools are responsible for and demonstrate accountability with the UK GDPR.

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.

Each School has appointed a Data Compliance Officer, who will deal with all Data Subjects' requests and enquiries concerning the School's use of personal data and endeavour to ensure that all personal data is processed in compliance with this policy and current data protection legislation.

The Data Compliance Officers can be contacted as follows:

St Faith's School

Patricia Lefrancois
Email: gdpr@stfaiths.co.uk
Telephone: 01223 229496
Address: St Faith's School, Trumpington Road, Cambridge, CB2 8AG

The Leys School

Fiona Oliver
Email: compliance@theleys.net
Telephone: 01223 854861
Address: The Leys School, Trumpington Road, Cambridge, CB2 7AD

The Schools have appointed Judicium Consulting Limited as their Data Protection Officer (DPO).

Judicium can be contacted directly as follows:

Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines. 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 (DSAR), 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;
- UK 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.

Staff Responsibilities

All staff members have a duty to assist the School 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:

Requirement	Details
Security of Personal Data	Personal Data must be kept securely (e.g. in a locked environment, encrypted or password protected if it is electronic).
Removal of hard copy Personal Data	Hard copy Personal Data removed from the school site must be held securely and not left unattended in public places.
Disposal of hard copy Personal Data	Hard copy documents containing Personal Data must be disposed of securely in the designated confidential waste bins located across the School site.
Retention of Personal Data	Personal Data must be held in accordance with department retention guidelines for each of the Schools.
Access to Personal Data	Staff must only access Personal Data which they have authority to access and only for authorised purposes.
Allowing others to access Personal Data	Staff must only allow others to access Personal Data if they have appropriate authorisation.
Disclosure of Personal Data	Personal Data must not be disclosed orally, in writing or by any other means, either accidentally or otherwise to any unauthorised third party.

Data Subject Responsibilities

All Data Subjects (e.g. staff, pupils (as appropriate to their age), 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.

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 DSARs and data breaches made in connection with the services to the Schools.

Data Security
Please refer to the Schools' Information Security Policy.

Data Retention
The periods for which the Schools normally retain Personal Data are contained within their respective Data 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 Breach Policies. Data Subjects and/or any applicable regulator will be notified of a data breach, where we are legally required to do so.

Individuals should contact the Compliance Officer at the relevant School, if they know or suspect that a Personal Data breach has occurred and reference the Data Breach Policy; they should not attempt to investigate the matter themselves.

Transparency and Privacy Notices
The Schools will provide detailed, specific information to Data Subjects. This information will be provided through the Schools' privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a Data Subject can easily understand them. The Schools' privacy notices are tailored to suit the Data Subject and set out information about how the Schools use their data.

Whenever the Schools collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we will provide the Data Subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the School's contact details and how and why we will use, process, disclose, protect and retain Personal Data. This information will be provided within our privacy notices.

When Personal Data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the Data Subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form

understandable by those defined as "children" under the UK GDPR.

Privacy by Design

The Schools adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.
Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Schools take into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of Data Subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Schools conduct DPIAs for any new technologies or programmes being used by the Schools which could affect the processing of Personal Data. In any event, the Schools carry out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Audit

The Schools, through our DPO regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of Personal Data.

Training

The Schools will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

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.

Record Keeping

The Schools are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the Schools;
- The name and contact details of the DPO;
- Descriptions of the types of Personal Data used;
- Description of the Data Subjects;
- Details of the Schools' processing activities and purposes;
- Details of any third-party recipients of the Personal Data;
- Where Personal Data is stored;
- Retention periods; and
- Security measures in place.

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 which applies to parents, and former parents where the issue first arose when their child was a pupil (please see the Schools' Complaints Policies for more information, available on their respective websites).

If Data Subjects would like to take the matter further, they 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/.

Related Policies

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

- Information Security Policy
- Respective Privacy Notices
- Data Retention Policy/Guidelines
- Acceptable Use Policy (The Leys School)
- Network and Social Media Acceptable Use Policy (St Faith's School)
- Remote Working Policy
- Data Security Breach Management Policy

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.

Appendix 1 – Data Subject Access Requests

Under 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 (DSAR). 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.

This appendix provides guidance for staff members on how DSARs should be handled and for all individuals on how to make a DSAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the School of the following: -

(a) Confirmation that their Personal Data is being processed;
(b) Access to their Personal Data;
(c) A description of the information that is being processed;
(d) The purpose for which the information is being processed;
(e) The recipients/class of recipients to whom that information is or may be disclosed;
(f) Details of the School's sources of information obtained;
(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting them, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
(h) Other supplementary information.

How to Recognise a DSAR

A DSAR is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a Parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process Personal Data about them and, if so
- for access to that Personal Data
- and/or certain other supplementary information.

A valid DSAR can be both in writing (by letter, email, text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a DSAR and should be treated as such.

A Data Subject is generally only entitled to access their own Personal Data and not information relating to other people.

How to make a DSAR

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the Personal Data being requested. This allows the School to easily recognise that you wish to make a DSAR and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request. A form is provided at Appendix 2 which you may wish to use this to submit a DSAR.

What to do when you receive a DSAR

All DSARs should be immediately directed to the relevant Data Compliance Officer who should contact Judicium as Data Protection Officer (DPO) in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

Acknowledging the Request

When receiving a DSAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School would normally work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a DSAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of Personal Data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If

the School do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The School needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but 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. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the Personal Data of the data subject to the third party, then it should provide the information requested directly to the Data Subject. It is then a matter for the Data Subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a Parent, to have access to the child's Personal Data. Before responding to a DSAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the School is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a DSAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the Personal Data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their Parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the Personal Data directly to the child.

The School may also refuse to provide information to Parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee for responding to a DSAR

The School will usually deal with a DSAR free of charge. Where a request is considered to be manifestly unfounded or excessive, a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time period for responding to a DSAR

The School has one calendar month to respond to a DSAR. 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, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third-party requester, the written authorisation of the Data Subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

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

School Closure Periods

The School may not be able to respond to requests received during or just before longer school closure periods within the one calendar month response period. This is because the staff available to process the request may be limited. When we acknowledge the request, we will inform you of any expected delay. 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.

Information to be provided in response to a request

The individual is entitled to receive access to the Personal Data we process about them and the following information:

- the purpose for which we process the Personal Data;

- the recipients or categories of recipient to whom the Personal Data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his Personal Data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;
    - where the Personal Data has not been collected from the individual, any information available regarding the source of the data;
    - any automated decision we have taken about them together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the DSAR was made in writing in a commonly used electronic format.

The information that the School are required to supply in response to a DSAR must be supplied by reference to the Personal Data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the Personal Data between the time the request is received and the time the Personal Data is supplied if such amendment or deletion would have been made regardless of the receipt of the DSAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending Personal Data after the receipt of a DSAR. The School is not allowed to amend or delete data to avoid supplying the data.

How the Personal Data is located

The Personal Data the School need to provide in response to a DSAR may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;

- pensions data;
- share scheme information;
- insurance benefit information.

The School should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of third parties - exemptions to the right of access

There are circumstances where information can be withheld pursuant to a DSAR. These specific exemptions and requests should be considered on a case-by-case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose Personal Data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the Data Subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the School must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances the School may be exempt from providing some or all of the Personal Data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any Personal Data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

Legal professional privilege: The School do not have to disclose any Personal Data which is subject to legal professional privilege.

Management forecasting: The School do not have to disclose any Personal Data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any Personal Data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The School can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the School can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the School need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the School should contact the individual promptly and inform them. The School do not need to comply with the request until the fee has been received.

Record Keeping

A record of all DSARs shall be kept by the Data Compliance Officer. The record shall include the date the DSAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

Appendix 2 – Data Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. You may wish to complete this form if you wish to make a request for your Personal Data but this is not mandatory and you may submit your DSAR by another means. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We may require proof of your identity before we can process your DSAR, and we will advise you of this when we acknowledge your DSAR.

Section 1

Please fill in the details of the Data Subject (i.e., the person whose data you are requesting). If you are not the Data Subject and you are applying on behalf of someone else, please fill in the details of the Data Subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

Personal Information *If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*
Details:

Employment records: If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your job role, the department(s) in which you worked, dates of employment etc. Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the Data Subject).

If you are **NOT** the Data Subject, but an agent appointed on their behalf, you may need to provide evidence of your identity as well as that of the Data Subject and proof of your right to act on their behalf. The School will advise you if this is needed at a later stage.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	
What is your relationship to the data subject? (e.g., Parent, legal representative etc.)	

I am enclosing the following copy as proof of legal authorisation to act on behalf of the Data Subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what Personal Data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form by email to the relevant Data Compliance Officer:

St Faith's
Patricia Lefrancois
Email: gdpr@stfaiths.co.uk
Telephone: 01223 229496

The Leys School
Fiona Oliver
Email: compliance@theleys.net
Telephone: 01223 854861