St Angela's
URSULINE SCHOOL

GDPR POLICY

GDPR POLICY

St Angela's Ursuline School Data Protection Policy

Purpose

St Angela's is committed to being transparent about how it collects and uses the personal data of its pupils, parents and staff. As a school we are determined to meet our data protection obligations. This policy sets out the school's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to all pupils, parents, governors and stakeholders within the wider school. This policy applies to the personal data of job applicants, employees and former employees, referred to as HR-related personal data.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, 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, health, sex life or sexual orientation and biometric data.

Data protection principles

St Angela's processes personal data in accordance with the following data protection principles:

- processes personal data lawfully, fairly and in a transparent manner;
- collects personal data only for specified, explicit and legitimate purposes;
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- keeps personal data only for the period necessary for processing;
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

St Angela's believes in telling individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the school relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the school processes special categories of personal data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data.

The school pledges to update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate. Similarly, the school pledges to update any other personal information that may be held by the school on request.

Personal data is held in the individual's personal file (in hard copy or electronic format, or both), and on other encrypted/locked systems. This is true for all stakeholders. The periods for which the school holds all personal data are contained in its privacy notices to individuals and in accordance with the schools data protection retention schedule.

St Angela's keeps a record of its processing activities in respect of all personal data in accordance with the requirements of the General Data Protection Regulations (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

The use of images and/or data for a specified purpose

The school will always seek consent from an individual (and where applicable parents also) prior to the use of personal data and/or images for any purpose. We acknowledge that this consent may also be withdrawn at any time.

Subject access requests

Individuals (whether pupil, parent or any other stakeholder for which we may hold data) have the right to make a subject access request*. If an individual makes a subject access request, the school will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the school carries out automated decision-making and the logic involved in any such decision-making.

(*please note that for pupils below the age of 16 such a request would, in most cases, have to have the support of a parent/legal guardian)

To make a subject access request, the individual should send the request to datamanager@stangelas-ursuline.co.uk or use the school's form for making a subject access request which can be found on our website. 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.

The school will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The school will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the school is not obliged to comply with it. Alternatively, the school can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request 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 this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the school to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the schools legitimate grounds for processing data (where the school relies on its legitimate interests as a reason for processing data). This includes exercising 'the right to be forgotten';
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the schools legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to datamanager@stangelas-ursuline.co.uk

Data security

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

Where the school engages third parties such as Payroll (for Staff) or SIMS (for pupils & parents) 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 personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner 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 it has taken.

International data transfers

The school will never transfer personal data to countries outside the European Economic Area regardless of the current legal status of the UK with the European Union.

Individual responsibilities

Individuals are responsible for helping the school keep their personal data up to date. Individuals should let the school know if data provided changes, for example if an individual moves house (pupils & parents) or changes their bank details (staff).

Members of staff may have access, depending on their role, to the personal data of other individuals in the course of their employment in order to exercise their duties. Where this is the case, the school relies on staff to help meet its data protection obligations to students, parents and colleagues.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the school) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the schools premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- report data breaches of which they become aware to datamanager@stangelas-ursuline.co.uk immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the schools disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing pupil or staff data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The school will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.