HOLY FAMILY CATHOLIC SCHOOL

Data Processing for Employees POLICY

Date agreed	**November 2024**
Next review date	**November 2025 (or in line with Catholic Education Services (CES) / LBWF Changes)**

THE MISSION STATEMENT OF THE SCHOOL

Holy Family Catholic School is a Catholic community embracing the clear Christian values of respect, service and justice.

We are a family of many cultures sharing one faith.

We exist to educate young people towards excellence in all dimensions of their lives, recognising the uniqueness of each and the equality of all.

Data Processing policy for Employees

Table of Contents

1. Introduction

The School is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its 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 the personal data of job applicants, employees, [workers, contractors, volunteers, interns, apprentices] and former employees, referred to as HR-related personal data.

Definitions

"Personal data" is any information that relates to an 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.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

During the course of our activities we, [the school] will process personal data (which may be held on paper, electronically, or otherwise) about our staff and we recognise the need to treat it in an appropriate and lawful manner, in accordance with **the UK General Data Protection Regulation (UK GDPR)** and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.

2. Data protection principles

The school processes HR-related 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.
- The school processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The school keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The school keeps personal data only for the period necessary for processing.
- 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 will usually only process staff personal data:

- Where consent has been given.
- Where the processing is necessary to comply with the performance of a contract.
- Where the processing is necessary to comply with a legal obligation.
- Where the processing may be necessary to protect the vital interests of a data subject

The processing of special categories of personal data, or criminal records data, will only be carried out if explicit consent has been given, or if the processing is legally required for employment purposes.

The school will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the [employment, worker, contractor or volunteer relationship, or apprenticeship or internship] is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the school holds HR-related personal data is seven years from the start of the academic year after the end /termination of employment. The exception to this is any records relating to potential safeguarding issues, which will be archived indefinitely.

The school keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the **UK General Data Protection Regulation (UK GDPR).**

3. Individual rights

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

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the school will tell him/her:

- whether or not his/her 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 his/her 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 his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and

- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The school will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

Where an individual wishes to exercise his/her rights to subject access, this will be dealt with under the schools Subject Access Request Policy and Procedure.

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 organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- 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 organisation's legitimate grounds for processing data.

To ask the school to take any of these steps, the individual should send the request to a.sabri@holyfamily.waltham.sch.uk

4. Data security

The school takes the security of HR-related 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 data is not accessed, except by employees in the proper performance of their duties

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.

5. Impact assessments

Some of the processing that the school carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the school will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

The school reserves the right to conduct routing monitoring of IT systems and e-mail accounts in line with the IT Acceptable Use Policy/Guidance. For all intents and purposes, work e-mail addresses are considered personal data, however the contents of the e-mails belongs to the school and as such will be subject to monitoring.

6. Data breaches

If the school discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will take all the necessary steps to remedy that breach as highlighted in the Schools Personal Data Breach Procedure.

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.

7. International data transfers

The school will not transfer HR-related personal data to countries outside the EEA.

8. 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 to the school changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals in the course of their [employment, contract, volunteer period, internship or apprenticeship]. Where this is the case, the school relies on individuals to help meet its data protection obligations to staff.

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 internal or third party) 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 school's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which

will be dealt with under the school's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

9. Training

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

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.

For help or advice on this policy please contact:

Maryline Alvis
Education Data Protection Officer via
Education Data Protection Service Team
Governance & Law
London Borough of Waltham Forest
Email: edposervice@walthamforest.gov.uk

Or

Ayesha Sabri
Data Protection Officer for Holy Family Catholic School