

Hazelwick School

Data Protection Policy

Date of publication	25th May 2018
Review date	25th May 2021

Introduction

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

Hazelwick School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Hazelwick School is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The school must be able to demonstrate compliance. Failure to comply with the Principles exposes the school and staff to civil and criminal claims and possible financial penalties.

Details of the school's purpose for holding and processing data can be viewed on the data protection register: <https://ico.org.uk/esdwebpages/search>

Hazelwick Schools registration number is [**Z3160198**]. This registration is renewed annually and up dated as and when necessary.

Aim

This Policy will ensure that:

- the school processes personal data fairly and lawfully and in compliance with the Data Protection Principles
- all staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy
- the data protection rights of those involved with the school community are safeguarded
- there is confidence in the school's ability to process data fairly and securely

Scope

This Policy applies to:

- personal data of all Hazelwick School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the school
- the processing of personal data, both in manual form and on computer
- all staff and governors

The Data Protection Principles

Hazelwick School will ensure that personal data will be:

- processed fairly, lawfully and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- accurate and, where necessary, kept up to date.
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Hazelwick School will be able to demonstrate compliance with these principles.

The school will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with
- to access their data
- to rectification of the record
- to erasure
- to restrict processing
- to data portability
- to object to processing
- not to be subject to automated decision-making including profiling

Roles and Responsibilities

The Governing Body of Hazelwick School and the Headteacher are responsible for implementing good data protection practices and procedures within the school and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy.

A designated member of staff, the Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the Headteacher.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, and data security breaches. Complaints about data processing will be dealt with in accordance with the school's Complaints Policy.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the school's Acceptable IT Use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT Use Policy.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

<https://irms.org.uk/page/SchoolsToolkit>

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.

Hazelwick School will have in place a data breach security management process and serious breaches, where there is a high risk to the rights of the individual, will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don't's in relation to data security in Appendix A.

Subject Access Requests

Requests for access to personal data (Subject Access Requests)(SARs) will be processed by the Data Protection Officer. Those making a Subject Access Request will be charged a fee in accordance with Regulations. Records of all requests will be maintained.

The school will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time limit is one calendar month of receipt of the request.

Sharing data with third parties and data processing undertaken on behalf of Hazelwick School.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the school e.g. by providing cloud based systems or shredding services, the school will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read the Acceptable IT Use Policy, AUP.

The school advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the school website.

The school also provides a Privacy Notice to staff which is available on the website.

The school will ensure Privacy Notices contains the following information:

- contact Data Controller and Data Protection Officer
- purpose of processing and legal basis
- retentions period
- who we share data with
- right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable

Photographs, Additional Personal Data and Consents

Where Hazelwick School seeks consents for processing personal data such as photographs at events it will ensure that appropriate written consents are obtained. The consent forms provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from parents/carers.

Appendix A

Staff will do the following:

- ☺ save all students data on the network
- ☺ use Foldr. for remote access of the network, making sure to save back on the network and not on personal computers
- ☺ email links to the folder on the network where student data is saved when sharing data with other members of staff
- ☺ place paper copies containing student data in the confidential shredding waste
- ☺ make sure that emails are addressed to the correct participant/s before sending
- ☺ consider the possible implications of student data being lost or misused and if you are unsure of what to do, stop and ask Joe Hillier, Data Protection Officer (DPO)
- ☺ immediately pass on details of any data breach to Joe Hillier, Data Protection Officer (DPO)

Staff will not do the following:

- ☹ use the same password for school and personal accounts
- ☹ use school emails for personal use
- ☹ use memory sticks or portable hard drives
- ☹ give anyone access to your password/s
- ☹ print then file student data from the network or save copies off the network
- ☹ email large amounts of personal data in an attachment
- ☹ place paper copies containing student data in the bin
- ☹ record unnecessary data in mark books
- ☹ leave sensitive data out in classrooms and offices – this should be locked away
- ☹ use SMW to send whole class lists where parents/carers are then given access names and information about other students in the class

