Data Protection

Reviewed by	Josie Payne (Head Teacher)
Review Frequency	May - Annually
Approval	FGB
Approved	May 2025
Next review due	May 2026

Glenwood School collects and uses personal information (referred to in the General Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information, this includes health information, details about recipients of pupil premium, employee references, safeguarding information about an individual and exam pupil references and results.
The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer (Liz Grady), who may be contacted at Glenwood School 01243 373120.

The school issues Privacy Notices (also known as Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

To be read and applied in conjunction with Hampshire Schools Retention Schedule.

Purpose
This policy sets out how the school deals with personal information correctly and securely and in accordance with the General Data Protection Regulations (GDPR), and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information data?
Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data and an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Glenwood school does not collect or use any biometric data.

Data Protection Principles

The UK GDPR establishes six principles as well as a number of additional duties that must be complied with at all times:

1. **Lawfulness, fairness and transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner. In order for personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include (amongst other relevant conditions) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority exercised by the school.
Where the special categories of personal data are processed, this shall include (amongst other relevant conditions) where processing is necessary for reasons of substantial public interest.
When processing personal data and special category data in the course of school business, the school will ensure that these requirements are met where relevant.

2. **Purpose limitation.** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes). The school will only process personal data for specific purposes and will notify those purposes to the data subject when it first collects the personal data or as soon as possible thereafter.

3. **Data minimisation**. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive. Personal data which is not necessary for the purpose for which it is obtained will not be collected.

4. **Accuracy.** Personal data shall be accurate and where necessary, kept up to date; Personal data should be reviewed and updated as necessary and should not be retained unless it is reasonable to assume that it is accurate. Individuals should notify the school of any changes in circumstances to enable records to be updated accordingly. The school will be responsible for ensuring that updating or records takes place where appropriate.

5. **Storage limitation.** Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for

which the personal data are processed. The school will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take reasonable steps to destroy or erase from its systems all data which is no longer required.

6. **Integrity and confidentiality**. Personal data shall be processed in a manner that ensures appropriate security of the personal data and which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Duties

Personal data shall not be transferred to a country or territory outside the UK and the European Union (EU)/European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Data Protection Impact Assessments (DPIA) and privacy notices

Data Protection Impact Assessments (DPIA) are reviewed and updated annually in order to reflect the school's way of working and to follow HCC policies and protocol.

Commitment

The school is committed to maintaining the principles and duties in the UK GDPR at all times. Therefore, the school will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this.
- Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.

- If the school plans to transfer personal data outside the UK and the EU/EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests).
- Ensure that personal information is not transferred outside the UK and the EU/EEA without the appropriate safeguards.
- Ensure that all staff and governors are aware of and understand these policies and procedures.

- Ensure that on the school social media page (Facebook), no photos of children, individuals details or other personal information is shared on this platform.

Retention and Disposal of Personal Data

The school will dispose of personal data in a way which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) as appropriate.

The school maintains a Retention Schedule that is specific and relevant to the specific types of information retained. The schedule outlines the appropriate periods for retention in each case.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Liz Grady at Liz.Grady@glenwood.hants.sch.uk, who will also act as the contact point for any Subject Access Requests.

Data breaches - Notification to the ICO

What responsibilities does the school have in relation to a personal data breach?

The school is required by the GDPR to report certain types of personal data breach to the Information Commissioner's Office (ICO).

When a personal data breach has occurred, the school will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then the school must notify the ICO; if it's unlikely then the school doesn't have to report it.

The school must report a notifiable breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

Communication with the affected individuals

The school is required by the GDPR to inform the affected individual(s) of certain types of personal data breach.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR requires the school to inform those concerned directly and without undue delay i.e. as soon as possible.
In addition to informing the individual about the nature of the personal data breach the school must provide them with information about:

- The name and contact details of our DPO for any queries
- The likely consequences of the personal data breach
- The measures taken/to be taken to address the breach including where appropriate measures to mitigate the possible adverse effects

The school might not be required to notify the affected individual if certain exceptions apply.

Record keeping

The school will keep a record of any personal data breaches whether they are notifiable to the ICO or not including the facts of the personal data breach, its effects and the remedial action taken.

Educational record request

- The Data Protection Officer - must answer an educational record request within 15 school days, not including bank holidays or inset days

- An ERR is a parent's right to access their child's educational record. The educational record will include the curricular record and also other information about the child that may be kept by the school e.g. details of behaviour and family background. The record will include information about the child created or provided by HCC employees, the school (or previous schools), the parent or child. (An ERR will cover handwritten notes made by staff except for lesson plans created just for their own use). The scope is narrower than a SAR.

- The ICO has no oversight over educational record requests. These requests are the direct right of the parent under the Education (Pupil Information) (England) Regulations 2005.

- In the case of an older child, there is no requirement to seek child consent to share information with the parent.

Subject Access Requests

- SAR'S can be directed to any member of staff (and not just the responsible party). There is a requirement for staff members to forward any subject access requests received to the responsible party within 24 hours.

- The Data Protection Officer - must answer a SAR within a calendar month, although this can be extended by up to two further months for complex requests.

- The scope is slightly wider. A SAR also enables access to the personal data a school processes that does not fall into the definition of an educational record. For example, records about the child created outside the HCC family e.g. police, NHS, private E.P, employees of other local authorities etc.

- The ICO is the regulator and the individual making the SAR can complain to the ICO if they do not agree with your response.

- It is the individual's right to make a SAR regarding their own personal data. Parents can only submit a SAR for information about their child if the child is not competent to act on their own behalf or has given their consent. On receipt of a SAR the DPO must therefore consider if the child has sufficient maturity to understand their information rights. A child of around the age of 12 is usually considered sufficiently mature. If the child has sufficient maturity, you can only proceed with the SAR if the child provides consent/authorises to share their information with the parent making the request.