General Data Protection Regulation

The Old School Henstead

2026 2027

Reviewed : September 2026	
Reviewed by D.Speakman	
To be reviewed by September 2027:	
Version	1

Data Protection Policy (*UK General Data Protection Regulation and Data Protection Act 2018*)

Purpose

The Old School Henstead collects and uses personal information about staff, pupils, parents 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.

Schools have a duty to *pay the data protection fee to and register with* the Information Commissioner's Office (ICO) *as a Data Controller, under the Data Protection (Charges and Information) Regulations 2018*, detailing the information held and its use. These details are then available on the ICO's website.

Legal Context

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with *the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, including Article 6 (Lawfulness of processing) and Article 9 (Processing of special categories of personal data)*.

It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data that relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The UK GDPR sets out six enforceable principles that must be adhered to at all times, together with an overarching accountability principle:

- Lawfulness, fairness and transparency – processed lawfully, fairly and in a transparent manner.
- Purpose limitation – collected for specified, explicit and legitimate purposes.
- Data minimisation – adequate, relevant and limited to what is necessary.
- Accuracy – accurate and, where necessary, kept up to date.
- Storage limitation – kept for no longer than is necessary.
- Integrity and confidentiality – processed securely, including protection against unauthorised or unlawful processing and against loss, destruction or damage.
- Accountability – the school must be able to demonstrate compliance with the above principles.

Privacy Notice and Transparency (Article 13)

In line with Article 13 UK GDPR, the school's privacy notice(s) for staff, pupils and parents will clearly set out: the identity and contact details of the Data Controller; the contact details of the Data Protection Officer; the

purposes and lawful basis for processing; the categories of personal data concerned; recipients or categories of recipients of the data; details of any transfers outside the UK and the safeguards applied; retention periods, or the criteria used to determine them; and the existence of individuals' rights, including the right to access, rectify, erase or restrict processing, the right to object, the right to data portability (where applicable), and the right to lodge a complaint with the ICO. Privacy notices will be reviewed alongside this policy and updated whenever processing activities change.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for advising on data protection obligations, monitoring compliance, providing advice on Data Protection Impact Assessments, and acting as the first point of contact for the ICO and for individuals whose data is processed by the school. The DPO's contact details are published in the school's privacy notices. Where the school relies on an exemption from the requirement to appoint a DPO, the basis for that decision will be documented and made available on request.

Lawful Basis for Processing

The school will identify and document the lawful basis under Article 6 UK GDPR (and, where special category or criminal offence data is processed, the applicable Article 9 or Article 10 condition) for each processing activity before that processing begins. Lawful bases are recorded in the school's Record of Processing Activities and referenced in the relevant privacy notice. Where consent is relied upon, it will be freely given, specific, informed and unambiguous, and individuals will be able to withdraw it at any time.

Records of Processing Activities (Article 30)

The school maintains a Record of Processing Activities (ROPA) in accordance with Article 30 UK GDPR, setting out the purposes of processing, categories of data subjects and personal data, categories of recipients, retention periods and a general description of technical and organisational security measures. The ROPA is reviewed at least annually and whenever a new or materially changed processing activity is introduced.

Data Protection Impact Assessments (DPIA)

Where a new project, system or process is likely to result in a high risk to the rights and freedoms of individuals — for example, the introduction of new technology, large-scale processing of special category data, or systematic monitoring — the school will carry out a Data Protection Impact Assessment before processing begins. The DPIA will identify and assess risks and the measures in place to mitigate them, and will be reviewed by the Data Protection Officer. Where residual high risk remains, the school will consult the ICO before proceeding.

Processors and Third-Party Assurance (Article 28)

Where the school engages a third-party processor to handle personal data on its behalf (for example, a cloud service, payroll or MIS provider), it will only do so where the processor provides sufficient guarantees of appropriate technical and organisational measures. A written contract compliant with Article 28 UK GDPR will be in place with every processor, covering the subject matter, duration, nature and purpose of processing, the processor's obligations regarding confidentiality, security, sub-processing, assistance with data subject rights, deletion or return of data at the end of the contract, and cooperation with audits. Due diligence on processors will be carried out before engagement and periodically thereafter.

Data Retention

Personal data will not be retained for longer than is necessary for the purpose(s) for which it was collected. Retention periods for all categories of data held by the school are set out in the school's Data Retention Schedule, which forms part of this policy by reference and is available from the Head or the Data Protection Officer. Data due for disposal will be securely and permanently destroyed in line with that schedule.

International Transfers

The school does not routinely transfer personal data outside the United Kingdom. Where a transfer outside the UK is necessary (for example, use of an overseas-hosted service provider), the school will only make that transfer where the destination is covered by UK adequacy regulations, or where appropriate safeguards are in place, such as the International Data Transfer Agreement (IDTA) or UK Addendum to the EU Standard Contractual Clauses. Details of any such transfers and safeguards will be set out in the relevant privacy notice.

Implementation

The Head will ensure that members of staff are aware of the Data Protection (*UK GDPR*) policy and its requirements including breach procedure. This will be undertaken as part of induction. If members of staff have any queries in relation to the policy, they should discuss this with the Head *or the Data Protection Officer*.

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary, in line with the school's Data Retention Schedule
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded, including encryption of data at rest and in transit, multi-factor authentication (MFA) for access to school systems holding personal data, strong and regularly updated passwords, and up-to-date cyber security controls such as firewalls, anti-malware software and staff cyber-awareness training
- Share information with others only when it is legally appropriate to do so, and only with processors bound by an Article 28-compliant contract
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than annually. The policy review will be undertaken by the Head or nominated representative, *i*n consultation with the Data Protection Officer.

Contacts

If you have any enquires in relation to this policy, please contact the Head on 01502 741150 who will also act as the contact point for any subject access requests, together with the school's Data Protection Officer. Further advice and information is available from the Information Commissioner's Office, ico.org.uk or telephone 0303 123 1113.

Procedures for Responding to Subject Access Requests

(Under the Data Protection Act 2018 and UK GDPR)

Rights of Access to Information

There are two distinct rights of access to information held by schools about pupils.

- Under *the* UK GDPR and the Data Protection Act 2018 any individual has the right to make a request to access the personal information held about them.
- The right of those entitled to have access to curricular and educational records. These procedures relate to subject access requests made under the UK GDPR and the Data Protection Act 2018.

Actioning a Subject Access Request

1. Requests for information must be made in writing; which includes email, and be addressed to the Head or the Data Protection Officer. If the initial request does not clearly identify the information required, then further enquiries will be made. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive, or provide a further copy of the same information. Alternatively, we may refuse to comply with the request in such circumstances.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address

also

- Birth / Marriage certificate
- P45/P60
- Credit Card or mortgage statement

This list is not exhaustive.

3. The response time for subject access requests, once officially received, is one calendar month from the date the request is received (or from receipt of any clarification requested, and, for identity verification, from confirmation of identity). This may be extended by a further two months where the request is complex or numerous, in which case the requestor will be informed of the extension and the reasons for it within one month of receipt.

4. The UK GDPR and Data Protection Act 2018 allow exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

5. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained.

6. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

7. If there are concerns over the disclosure of information then additional advice will be sought from the Data Protection Officer.

8. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

9. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

10. Information can be provided at the school with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaints procedure. Complaints which are not appropriate to be dealt with through the school's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these procedures then please contact Mrs Sonn, senior teacher, responsible for Data Protection. Further advice and information can be obtained from the Information Commissioner's Office, *ico.org.uk*.

Data Protection Breach

Data held by the School is both personal and sensitive. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, the school will take appropriate action to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by The Old School Henstead.

This breach procedure sets out the course of action to be followed by all staff if a data protection breach takes place.

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- loss or theft of pupil, staff or governing body data and/or equipment on which data is stored
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- hacking *or other cyber security incidents (e.g. phishing, ransomware)*
- 'Blagging' offences where information is obtained by deception

Immediate Containment/Recovery

On discovery of a data protection breach, the following steps will be followed:

1. The person who discovers/receives a report of a breach must inform the Head or, in their absence, a member of SLT *and the Data Protection Officer*. If the breach occurs or is discovered outside normal working hours, this will begin as soon as is practicable.

2. The Head (or nominated representative) will ascertain whether the breach is still occurring. If so, steps will be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff.

3. The Head (or nominated representative) will inform the Chair of Governors as soon as possible. It is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head (or nominated representative) will also consider whether the Police needs to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5. The Head (or nominated representative) will quickly take appropriate steps to recover any losses and limit the damage.

Steps might include:

- Attempting to recover lost equipment
- The use of back-ups to restore lost/damaged/stolen data
- If bank details have been lost/stolen, the bank contacted directly for advice on preventing fraudulent use
- If the data breach includes any entry codes or IT system passwords, then these will be changed immediately*, multi-factor authentication reviewed,* and the relevant agencies and members of staff informed

Investigation

In most cases, the next stage would be for the Head (or nominated representative*, together with the Data Protection Officer*) to fully investigate the breach. The Head (or nominated representative) will ascertain whose data were involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

The investigation will consider:

- the type of data
- its sensitivity
- what protections are in place (e.g. encryption*, access controls*)
- what has happened to the data
- whether the data could be put to any illegal or inappropriate use
- how many people are affected
- what type of people have been affected (pupils, staff members and suppliers) and whether there are wider consequences to the breach

A clear record will be made of the nature of the breach and the actions taken to mitigate it *in the school's breach log/register*. The investigation will be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements will be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place. The Head (or nominated representative), after seeking expert or legal advice from the Data Protection Officer, will decide whether anyone should be notified of the breach. In the case of significant breaches likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office (ICO) will be notified within 72 hours of the school becoming aware of the breach*,* in accordance with Article 33 UK GDPR.

Incidents will be considered on a case-by-case basis. The following points will help the Head (or nominated representative) to decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?
- If a large number of people are affected, or there are very serious consequences, the ICO should be notified if personal data is involved.

Further guidance is available from the ICO on when and how to notify them, at ico.org.uk.

The notification will include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to mitigate the risks posed by the breach. When notifying individuals, specific and clear advice on what they can do to protect themselves and what the school are willing

to do to help them. An opportunity to make a formal complaint if individuals wish (see the School's Complaints Procedure) will be available.

Review and Evaluation

Once the initial aftermath of the breach is over, the Head (or nominated representative*, with the Data Protection Officer*) will fully review both the causes of the breach and the effectiveness of the response to it. It will be written and placed on the agenda of the next Senior Leadership Team meeting for discussion. If systemic or ongoing problems are identified, then an action plan will be drawn up to put this right. If the breach warrants a disciplinary investigation, the Head (or nominated representative) will action this. Consideration will be given to reviewing this breach procedure whenever the data protection policy is reviewed.