General Data Protection Regulation

The Old School Henstead

Written by:	WJM
Last reviewed on:	9 September 2022
Next review due by:	9 September 2023

Policy 22: Data Protection Policy (General Data Protection Regulation)

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 be registered, as Data Controllers, with the Information Commissioner's Office (ICO) 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 Data Protection Act 1998, and other related legislation as stated in Article 6 EU GDPR Lawfulness of processing, and Article 9 EU GDPR 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 Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:
1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes; 3. Personal data shall be adequate, relevant and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Implementation

The Headmaster will ensure that members of staff are aware of the Data Protection (General Data Protection Regulation) policy and its requirements including breach procedure. This will be undertaken as part of induction and will be included on the

agenda of every new term staff meeting agenda. If members of staff have any queries in relation to the policy, they should discuss this with the Headmaster.
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
- 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
- Share information with others only when it is legally appropriate to do so
- 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 Headmaster or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Headmaster on 01502 741150 who will also act as the contact point for any subject access requests. Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453

Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.
1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records. These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Headmaster. 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. 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

- 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 30 days (working school days). However, the 30 days will not commence until after receipt of clarification of information sought.
4. The Data Protection Act 1998 allows 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.
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 Miss Melissa Clifton, Deputy Head, responsible for Data Protection.
Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Guidance: http://www.ictknowledgebase.org.uk/dataprotectionpolicies
http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

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
- '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 Headmaster or, in his absence, the Deputy Head. If the breach occurs or is discovered outside normal working hours, this will begin as soon as is practicable.

2. The Headmaster (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 Headmaster (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 Headmaster (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 Headmaster (or nominated representative) will quickly take appropriate steps to recover any losses and limit the damage.
Steps might include:
a. Attempting to recover lost equipment.
b. The use of back-ups to restore lost/damaged/stolen data.
c. If bank details have been lost/stolen, the bank contacted directly for advice on preventing fraudulent use.
d. If the data breach includes any entry codes or IT system passwords, then these will be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Headmaster (or nominated representative) to fully investigate the breach. The Headmaster (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)
- - 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. 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 Headmaster (or nominated representative), after seeking expert or legal advice, will decide whether anyone should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) will be notified with 72 hours of the breach.
Incidents will be considered on a case by case basis. The following points will help the Headmaster (or nominated representative) to decide whether and how to notify:

a. Are there any legal/contractual requirements to notify?
b. Will notification help prevent the unauthorised or unlawful use of personal data?
c. Could notification help the individual – could they act on the information to mitigate risks?
d. 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 available from the ICO on when and how to notify them, which can be obtained at: http://www.ico.gov.uk/for_organisations/data_protection/the guide/~/meia/documents/library/Data_Protection/Practical_application/breach_reporting.ashx.) C
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 Headmaster (or nominated representative) 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 these right. If the breach warrants a disciplinary investigation, the Headmaster (or nominated representative) will action this. Consideration will be given to reviewing this breach procedure whenever the data protection policy is reviewed.