Table of Contents

Aims

Woodford County High School is obliged to collect and use personal information about current, past and prospective employees, governors, students, parents, guardians, suppliers and other third parties who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions.

The purpose of this policy is to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation. 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.

Woodford County High School will take all reasonable steps to process personal information in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this Policy, any reference to students includes current, past or prospective students.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities as detailed in this Policy.

Statutory Requirements

UK General Data Protection Regulations (GDPR) May 2018

UK General Data Protection Regulation (GDPR)

UK General Data Protection Regulation replaces the previous Data Protection Directives that were in place. It was approved by the EU Parliament in 2016 and comes into effect on 25th May 2018.

GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that an individual's data should not be processed without their knowledge but only with their 'explicit' consent. GDPR covers personal data relating to individuals. Woodford County High School is committed to protecting the rights and freedoms of individuals with respect to the processing of children's, parents', visitors' and staff personal data.

The General Data Protection Regulation gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly

General Data Protection Principles

GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Data Protection Controller

All schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. This information is then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all students and parents; this summarises the information held on students, why it is held and the other parties to whom it may be passed on.

Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and for providing advice and guidelines where applicable. The school's Data Protection Officer is Fiona Alderman (LBR) contact email DPO@woodford.redbridge.sch.uk.

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals or If they need help with any contracts or sharing personal data with third parties

Staff must only process personal data where it is necessary in order to do their job

When staff no longer need the personal data they hold, they must ensure it is deleted/shredded or pseudonymous. This will be done in accordance with the Records Management Society's Retention Guidelines for Schools.

What is Personal Information?

Personal information is information that the School collects about staff, pupils and parents. This includes information such as name, date of birth, National Insurance Number, address as well as exam results, medical details, nationality and behaviour records. The School may also record religion and ethnicity.

Definitions:

Personal Data: personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by:

- reference to an identifier such as a name,
- identification number,
- location data,
- an online identifier
- It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity

Special categories of personal data: Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing: Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject: The identified or identifiable individual whose personal data is held or processed.

Data Controller: A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

School Site Procedures & Data Security

GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if said third party agrees to comply with those procedures and policies, or puts in place adequate measures themselves. Woodford County High School will take all reasonable steps to ensure that members of staff will only have access to personal data relating to students, their parents or guardians where it is necessary for them to do so. Woodford County High 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 or legally required
- 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 (paper files or on our computer system)
- Share personal information with others only when it is necessary and legally appropriate to do so
- Set out clear procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests in the UK General Data protection regulation
- Train our staff so that they are aware of and understand our policies and procedures

All staff will be made aware of this policy and their duties under the UK General Data Protection Regulation and the school will ensure that all personal information is held securely and is not accessible to unauthorised persons and will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

Security procedures include:

1. The school has electronic gates installed
2. We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
3. The school operates a key fob entry system
4. Equipment - data users should ensure that individual monitors do not show confidential information to passers-by and that they log off / or lock their PC when it is left unattended.

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular

1. Secure lockable desks and cupboards - desks and cupboards are kept locked if they hold confidential information of any kind (personal information is always considered confidential).
2. Methods of disposal - paper documents are shredded or placed in dedicated confidential document bins located around the site, date storage devices are physically destroyed when they are no longer required
3. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
4. Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are prompted to change their passwords every 90 days.
5. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
6. Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT Acceptable Use Policy).
7. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Providing Information to Third Parties

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us

In particular they should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;
- Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;
- Refer to the head teacher for assistance in difficult situations;
- Where providing information to a third party, do so in accordance with the data protection principles.

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. So it is important to establish whether the information requested falls within the definition of personal data. In most cases, it will be obvious whether the information being requested is personal data, but we have produced separate guidance to help you decide in cases where it is unclear: *Determining what is personal data (pdf).* Please also see the key definitions.

Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

This includes:

- confirmation that you are processing their personal data
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- They can request rectification, erasure or restriction or to object to such processing;
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

    - Name of individual
    - Correspondence address
    - Contact number and email address
    - Details of the information requested If staff receive a subject access request they must immediately forward it to the SRO

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO

Links with other policies

This data protection policy is linked to the following school policies:
SP04.04Freedom of Information Publication Scheme
SP03.04ICT Acceptable Use Policy (Staff/Student/parents)
SP04.01Safeguarding and Child Protection Policy
SP03.07ICT eSafety Policy
SP02.11Staff Code of Conduct

Complaints

Complaints will be dealt with in accordance with the school's Complaints Policy (SP05.07). Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Further advice and information is available from the Information Commissioner's Office:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

Approval/Amendment

This policy is approved by the Governing Body of Woodford County High School. Any Amendments to this Policy will be updated as necessary to reflect best practice or amendments made to the UK General Data Protection regulations and will require approval by the Governing Body of Woodford County High School.

Questions

If you have any questions about this present statement of policy, please contact the School Business Manager at Woodford County High School, High Road, Woodford Green, Essex, IG8 9LA, who will also act as the contact point for any subject access requests.

Further advice and information, including a full list of exemptions, is available from the Information Commission, www.informationcommissioner.gov.uk