

Data Protection Policy

Summary

Woodham Academy is a forward-looking school dedicated to giving all young people the best possible start in an increasingly competitive and rapidly-changing world. We are determined that all of our students will develop the broad skills set, including high standards of ICT, needed to progress into employment, further education or training.

As a school our staff are constantly developing and sharing good practice. ICT is increasingly used to support the professional work of staff, and enhance the management and administration of the school. The development of our Virtual Learning Environment and other online services are allowing our staff, students, parents/carers, other stakeholders and the wider community, to access resources, information and communications from home.

Alongside this determination to progress the use of new and existing technologies, is our recognition of the need for responsible and careful management of data, ICT access and resources. Application of this policy will allow us to fulfil our obligations as outlined in the Data Protection Act (1998), and therefore protect the rights and privacy of our staff, students and key stakeholders.

Date adopted	November 2009
Review date	Annually
Last Reviewed	May 2017

1. Principles:

This policy is based upon the following principles:

- We are committed to promoting a technological culture
- Staff, students and all school stakeholders have a right to expect that the school will comply with the principles of the Data Protection Act (1998) including, but not exclusively, the following:
 - Recruitment and payment of staff
 - Administration of programmes of study, schemes of work and lesson plans
 - Student details including personal details, SEN information, attendance, behaviour records, and attainment and progress data
 - Complying and responding to requests from DCSF and the LA in providing data returns

This policy should be read alongside the schools ICT User Policy, Safeguarding Policy, and staff Code of Conduct. A brief staff guide of this data protection policy has also been produced to support all staff in fulfilling their duties whilst ensuring compliance with the Data Protection Act (DPA).

2. Aims of the policy

Specifically, this policy will:

- Outline the responsibilities as specified by the DPA
- Outline the principles of the DPA
- Give guidance on responsible access to and use of data within school
- Give guidance to staff who wish to access student or staff data remotely
- Outline how the school will manage internet access for staff, students and other stakeholders
- Give guidance on the use of email
- Outline how the portal and VLE can be used appropriately by staff, students and other stakeholders

3. Definitions and responsibilities

Woodham Academy is the “data controller” under the terms of the DPA. The Headteacher is responsible for ensuring that day-to-day data protection matters are managed through the organisational, physical and intellectual deployment of staff and resources. The Headteacher also maintains responsibility for ensuring that the notification on the Information Commissioners website is kept up to date and accurate. Data subjects are individuals – staff, students or stakeholders who provide the school with information. Data subjects who provide the school with data are responsible for ensuring that the information is accurate and up to date. Compliance with the legislation is the responsibility of everyone within or associated with the school who process data or personal information.

4. Principles of the DPA

The Data Protection Principles require that the school will:

4.1 Process personal data fairly and lawfully

The school will make all reasonable efforts to ensure that data subjects are aware that the school is the data controller, the purpose of the data processing, any disclosures to third parties that can be foreseen, and an indication of the period of time for which the data will be kept, and other relevant information.

4.2 Process the data for the specific and lawful purpose for which it was collected, and not further process data in a manner incompatible with this purpose.

The school will ensure that the reason that the data was collected originally is the only reason for processing the data, unless the individual is informed of any additional processing before it takes place

4.3 Ensure that the data collected is adequate, relevant and not excessive in relation to the purpose for which it is processed.

The school will not collect any personal data which is unnecessary for the purpose for which it was obtained, and data collection forms will reflect this. Irrelevant or superfluous data will be destroyed.

4.4 Keep personal data accurate and up to date

The school reviews and updates all personal data held on a regular basis. It is the responsibility of the data subject to ensure that the data held is accurate and up to date. The school as data controller has the responsibility to ensure that any change notifications are noted and acted upon.

4.5 Keep personal data for the minimum necessary period

The school undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and other statutory requirements. Please see note below on disposal of data.

4.6 Process personal data in accordance with the rights of the data subject

See specifically Section 6 in addition to Section 4.

4.7 Put in place appropriate measures (both organisational and technical) against unauthorised or unlawful processing of data, and against accidental loss or destruction of data.

All staff are issued with their own personal log-in and password to the network and a separate one for the information management system (SIMS). The access rights of individual users are defined by the Leadership Group depending on their role within the school and implemented by the Data Manager. This supports the school in ensuring that data stored on SIMS is only accessed by those who should have access to the data to allow them to fulfil their duties.

Hard copies of personal data are kept in a secure room, in secure lockable filing cabinets.

PC screens used by staff or CCTV screens are placed so as not to be visible by anyone other than authorised persons, and PC screens are not left unattended without a password protected screen-saver. Where CCTV cameras operate around school prominent signs will inform people of their use to ensure compliance with the DPA.

4.8 Ensure that no personal data is transferred to a country or territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to processing data.

The school will not transfer data to territories or countries outside of the European Economic Area without the explicit consent of the data subject.

As our website is available worldwide, personal data such as photographs will only be placed on the website with prior consent of the data subject.

5. Consent as a basis for processing data

It is not always necessary to gain consent from individuals before processing their data, however it is considered good practice to ensure that data is collected and processed in an open and transparent manner. Consent will always be sought for processing any sensitive data. Routine consent issues will be incorporated into the school's student and staff data gathering sheets

6. Subject Access Requests

Every data subject has the right to access the personal data and information which relates to them, either on SIMS or within their paper records. Requests to see, or receive paper copies of school records, should be made in writing to the Headteacher. The school will respond within 15 school days, and a fee to cover copying costs may be charged as follows:

1 – 19 pages	£1
20 – 99 pages	£5
100 – 149 pages	£10
Over 150 pages	£20

The school reserves the right to withhold information that may cause harm to the physical or mental health of the data subject, information that may identify third parties (for example, other students), or information that forms part of court reports.

7. Disclosures

Personal data will only be disclosed to organisation or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

Personal data will only be disclosed to Police Officers with the authorisation from the Headteacher. In all circumstances the well-being and safety of our students and staff will form the basis for the decision to give authorisation or not.

The police only have legal powers to access information and data if it forms part of an investigation, and can not simply turn up and ask for information. However, the school may choose to seek a local agreement with the police – if so we will need to notify parents that this is the case.

8. Monitoring and Review

The systems will be monitored by the Data Manager to ensure compliance with the DPA and associated legislation. Any breaches of this policy or of the legislation must be reported immediately to the Deputy Headteacher who maintains line management responsibility for the Data Manager, Network Manager and therefore the implementation of this policy.