Woburn Lower School

Acceptable Use Policy for Adults

All staff and governors should be aware of this agreement, and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action. It is vital that the school fulfil its obligations under the General Data Protection Regulation (2018) and Freedom of Information Act (2000). All staff are given training on this, however this Acceptable Use Policy has been put together to ensure that all staff are aware of and follow specific rules.

Data to which this AUP applies

1. Personal data is defined as data with two or more personal identifiers (e.g. name and address, name and date of birth).

2. Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an unauthorised individual. For example SEN, racial or medical data, bank details, phone numbers.

3. This AUP also applies to other confidential data such as performance management documents.

Security of paper-based data

1. Staff are responsible for ensuring that data issued to them remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel e.g. students.

2. If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.

3. Data should never be taken outside of the EU.

4. Particularly sensitive data, e.g. SEN or medical records, payroll details etc, should never be removed from the school site and remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.

5. All paper based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).

Security of electronic data

1. Ensure that your passwords for access to the network, email, are strong passwords. You should change these on a regular basis, and not tell other members of staff or students your passwords.

2. Ensure that you lock or log out your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes place using your credentials, which can be monitored.

3. Ensure that data is not visible to students or other unauthorised personnel.

4. In general there should be no need to store data outside school.

5. If storing/transferring data using a removable device, this device must be an encrypted USB drive which will be supplied to you by the school on request. If lost report it immediately to the data Headteacher. This USB drive should remain physically secure both in transit and when stored, in the same way as paper based records. It must not be taken out of the EU. When your employment with the school terminates, you should return the USB drive to the Headteacher for safe disposal. Data must not be copied from the encrypted USB drive onto any computer equipment used off school site (this includes home computers).

6. Photos and videos of students must only be taken using school owned devices. Any exception to this can only be authorised by the Headteacher.

7. Files should be deleted from the network and encrypted USB drives when no longer needed, in line with the school's data retention schedule.

8. When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends.

Release of data to others

1. Staff may share information with each other regarding students as necessary in the performance of their duties, as long as this sharing of information is in the best interests of the students. The only exception to this is where a manager has explicitly stated that information is not to be shared.

2. When sharing data with another organisation e.g. another school, you should check the legitimacy of the potential recipient. Wherever possible, school-to-school student data transfers will be made by the admin staff using the secure site.

3. Staff with access to data regarding other staff, such as contracts and pay scales, should ensure they have been granted permission to access this data by the Headteacher.

4. You should use your school provided email account for all email related to your work for the school. All other emails and correspondence goes via the school email and through the office admin staff including the Headteacher.

5. The school takes any data breach very seriously. Should you become aware of any such breach, or the potential for one, you should inform a Headteacher.

Freedom of Information and Subject Access Requests

1. Any member of staff or the Governing Board may receive a subject access request for personal data, or a request for information under the Freedom of Information Act. Such requests will be made in writing or by email.

2. If you receive such a request, you should inform the Headteacher. The school has a legal duty to respond to requests within a time limit, so it is important that you pass on the request in a timely manner.

3. You should then await a response for the Headteacher before sending a response to the request.

4. Staff should be aware that, in fulfilling requests, the school may be required to disclose the contents of emails. It is therefore vital that staff remain professional in all correspondence.

5. It is an offence to wilfully conceal, damage or destroy information in order to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed.

Related policies:

Whistleblowing

E-safeguarding

Safeguarding

Staff Code of Conduct

Disciplinary Procedures

Data Protection

Governor Code of Conduct

Governor Statement of Behaviour

Governor:

Date:

Headteacher:

Date: February 2023

Review: February 2026