# Wootton Bassett Infants' School

# Staff Computer Policy

| | |
|---|---|
| Author: | WBIS |
| Approved Date: | September 2024 |
| Review Date: | September 2025 |
| Review Cycle: | 2 years |
| Approval Level: | HT |

Staff within the school have access to a wide range of sensitive information. There are generally two types of sensitive information: personal data concerning the staff and pupils and commercially sensitive financial data. It is important to ensure that both types of information are always managed in a secure way.

**Procedures and practice:**

The following practices will be applied within the school:

- The amount of data and photos held by the school should be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personal data held by the school will be securely stored and sent by secure means.

**Securing and handling data held by the school:**

The school will encrypt any data that is determined to be personal or commercially sensitive in nature. This includes fixed computers, laptops and memory sticks. Memory sticks should be scanned for viruses before any file stored is opened each time the stick is used.

Staff should **not** remove or copy sensitive data from the organisation or authorised premises unless the media is:

- encrypted,
- is transported securely
- will be stored in a secure location.

The school provides remote access to our system via a Secure VPN connection. The school also provides access to email via Outlook Web. Both of these methods are encrypted and secure connections. Where possible staff should use these methods when accessing confidential data, such as student records.

**Staff Declaration**

I confirm the following:

- Passwords that I use to access school systems will be kept secure and secret – if I have reason to believe that my password is no longer secure, I will change it.
- I acknowledge that the computer provided for me to use remains the property of the school and should only be used for school business.
- Any laptops will be returned to the school when I leave for the IT technician to wipe.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web content/Social Media or use pictures or text that can identify the school, without the permission of the Headteacher.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school. I will seek permission with the school's technician / Network Manager should I need to install additional software.

- I will always adhere to the copyright.

- I will always log off the system when I have finished working.
- I understand that the school may, in line with the filtering and monitoring guidelines monitor the internet sites I visit.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of admin / school technician / headteacher. Attachments should be scanned for virus infection before being opened.
- Any e-mail messages I send will not damage the reputation of the school.
- Any emails I send outside of the school will not contain any children personal details, only initials and DOB. Any documents will be sent password protected or via One Drive.
- All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be forwarded.
- I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
- I understand that I am responsible for the safety of school data that I use or access.
- Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. <u>This information must not be stored on a personal (home) computer.</u>
- Members of staff (e.g. senior administrators) who are given full, unrestricted access to an organisation's management information system should do so over an encrypted connection and use two-factor authentication, which is available to SIMS users from Capita. <u>This information must not be stored on a personal (home) computer.</u>
- In order to maintain the security of data I will take the following steps:
    - I will store data files in my user area on the school server only for as long as is necessary for me to carry out my professional duties.
    - I will not save data files to a PC or laptop other than that provided by the school.
    - If I need to transfer sensitive data files and no secure electronic option is available, I will only do so using the encrypted USB key provided by the school.
    - Sensitive data will only be sent electronically through a secure method, e.g., SecureNet Plus. If this is not available, then the minimum requirement is to password protect the document before attaching it to email.

      Sensitive data includes:

        - Pupil reports
        - SEN records
        - Letters to parents
        - Class based assessments
        - Exam results
        - Whole school data
        - Medical information

- Information relating to staff, e.g., Performance Management reviews.

If I am in any doubt as to the sensitivity of data I am using, I will consider these questions:

- Would disclosure / loss place anyone at risk?
- Would disclosure / loss cause embarrassment to an individual or the school?
- Would disclosure / loss have legal or financial implications?

If the answer to any of these questions is yes, then the data should be treated as sensitive.

I understand that if I do not adhere to these rules outlined in this policy, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow including notification to professional bodies where a professional is required to register. If an incident is an offence under the Computer Misuse Act or the Data Protection Act this may be reference for investigation by the Police and could recorded on any future Disclosure and Baring Services checks.