Minerva

Learning Trust

Portable Storage Media

Acceptable Use Policy (AUP)

Date First Published	April 2019
Version	1
Last approved	
Review Cycle	Annual

Contents

Changes to this edition

First edition.

The policy provides guidance to staff on the secure use of portable storage media for carrying information.

Portable storage media includes but is not limited to:

- CDs and DVDs
- USB Memory Sticks and External Hard Drives
- Memory Cards (e.g. SD Cards)
- Digital Cameras, MP3 Players, Mobile Phones

Responsibilities of Headteachers and Governors

Headteachers and or Governors will support this AUP by:

- Implementing the Policy within the school and ensuring that the AUP is circulated to all personnel
- Ensuring that staff understand the legal risk and security implications of improper use of portable data storage
- Promote good information security practice by, leading by example and ensuring they adhere to the conditions within this policy

Responsibility of Staff

All staff have a duty of care to ensure the requirements in this policy are adhered to.

The loss of any information including the loss of portable storage media is reportable under GDPR regulations. In the first instance, the loss of such must be reported to the Schools Business Manager who will then seek advice from the trusts GDPR representative.

Security Risks

Loss of information – portable storage media, like a computer, is susceptible to data loss or failure.

Potential breach of confidentiality – if the portable storage media is lost or stolen.

Corruption of data – can occur if the portable storage media is not removed from a computer properly.

Virus transmission – portable storage media can introduce viruses onto a computer network.

Data breach - If you leave your portable storage media connected to a PC, the next person to log on can access the data even if it's encrypted.

All the above are reportable under current GDPR regulations.

Avoidance

Confidential, Sensitive and Person Identifiable Data must not be stored or carried on portable storage media.

Staff should use other secure methods for accessing information such as Microsoft One Drive.

Passwords must not be stored with portable storage media in any circumstances.

Email is not secure and must not be used as a communication or data transfer mechanism for confidential, sensitive and person identifiable information. Microsoft One Drive can be used for such requirements.

Sensitive Information

The term 'Sensitive Information' is used in a variety of contexts and can have different meanings according to the relevant legislation or usage.

In the context of this Acceptable Use Policy, 'Sensitive Information' includes any information which requires protection from unauthorised or unwanted loss or disclosure.

This will typically include, but is not limited to:

- Personal Data (including pupil records, staff records, appraisals, disciplinary cases, etc.)
- Sensitive Personal Data (for example, health records)
- Bank and Payment Card information
- Commercial data, leases, contracts, etc.
- Any information where loss or disclosure could lead to damaging consequences for an individual or group of individuals; damage the reputation of the School, compromise ICT security or cause the school to not fulfil its statutory obligations

Encryption

In the first instance, any portable storage media will need to be wiped clean and encrypted by the ICT staff for first use.

Passwords must not be disclosed to other persons.

Monitoring

The school (and/or trust if applicable) does not generally engage in systematic monitoring and recording activities. However, it reserves the right to do so where there is reason to believe that misuse of information assets or computing facilities is occurring. Nevertheless, the school (and/or trust if applicable) maintains the right to examine any systems and inspect any data recorded in those systems, in order to ensure compliance with this policy. Staff should be aware that any breaches found may be investigated and could lead to disciplinary action.