endeavour
multi academy trust

TWO RIVERS HIGH SCHOOL

ICT Security Policy

Two Rivers School

Review date:	Autumn 2021 Logistics Committee
Next Review:	Autumn 2023

Rules and Agreements for Staff

Rules for ICT Users – Staff

The objective of this policy is to create and maintain a high level of importance of ICT and Data Security within the school. All staff have a responsibility to ensure proper use of equipment and data, both by themselves and the pupils they teach.

This policy is relevant to all ICT services and electronic communication methods irrespective of the equipment or facility in use. This applies to all employees and others using the school facilities either on or off the school premises.

Legislation

- The school and its staff must comply with all UK legislation affecting ICT. All school staff must comply with the following acts or they may be held personally responsible:

  Human Rights Act, 1998
  Copyright Designs and Patents Act 1988
  Computer Misuse Act 1990
  General Data Protection Regulations 2018

General Use

- Users of the system must comply with the requirements of the ICT Security Policy.
- ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held through complying with the school Privacy Notice.
- Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information.
- Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat and water damage.
- Computers logged onto must be locked when unattended.
- These same rules apply to official equipment used at home.
- All appropriate devices are password protected, and this password is changed on a regular basis.

Passwords

- If software packages come with pre-installed passwords these must be changed immediately after installation.
- Passwords must not be written down or shared unless this is unavoidable.

- Passwords should not be the same as a username or be easily guessed by anyone attempting to login.

Access Levels

- Members of staff will have access limited only to those systems or data which they require during their normal employment or educational activities. If special access is needed for a limited period access rights must be granted by the Executive Headteacher/Headteacher and removed after this period has expired.

Security Breaches

- Any staff member, or pupil that becomes aware of an actual or potential breach of security must report this to the Executive Headteacher/Headteacher.
- This must be recorded centrally and to the Data Protection Officer (DPO) who will advise the Information Commissioners Office (ICO).

Software

- Only software, for which the school holds a legitimate license, should be installed on any school computer by an authorised member of staff.
- The copying of proprietary software programs or associated copyrighted documentation is prohibited and is a criminal offence.

Viruses

- Software or files must not be loaded onto ICT equipment unless its source has been verified as legitimate and the software checked for viruses. This includes commercial "demos" software purchased for home use but used on school machines.
- If there are any doubts about the authenticity or content of an email or other electronic data or attachments these must be reported to the ICT Manager immediately. Any messages or communications which are suspicious must not be opened or loaded onto school equipment until they have been properly checked by an approved member of staff, i.e. the ICT Manager or Senior Leadership Team.
- Anti-virus software should be used to protect school equipment and data, presently this is TrendMicro.
- All storage media should be checked by the ICT Team and sensitive information should not be taken off site by use of memory sticks or laptops without the necessary security in place which is outlined in the GDPR Risk Assessment – shared with all staff.

Telephones

- Telephone users must always be aware of their surroundings and take these into account when carrying out any conversation. This is especially important where confidentiality is an issue.

Email

- Email facilities are provided primarily for business use. However, it is acknowledged that in some exceptional circumstances it may be permissible to respond to a private email. Regardless of this, school email facilities must never be used in connection with any secondary business activities
- Staff and pupil mailboxes and their contents may be examined by the school, Endeavour Multi Academy Trust, its auditors or any law enforcement agency. Due consideration of the provisions of the Human Rights Act and any other legislation will be made when undertaking such examinations
- Where necessary, attachments and sensitive documents should be password protected. Encryption should also be in place for the sending of sensitive emails.

Internet

- Access to the internet is provided primarily for appropriate educational use
- The school, Endeavour Multi Academy Trust, its auditors and any law enforcement agency may monitor the use of the internet and will report any irregularity to the school Local Governors. Use of the Internet is considered to be an expression of consent by the user to such monitoring, recording and auditing.
- Systems are in place to restrict access to potentially offensive material which will record any attempt to access unsuitable sites and material. These will be investigated and may lead to disciplinary action. In exceptional circumstances a referral to the police could be made. The schools use Smoothwall software.

Data Backup and Disaster Plan

- The school has systems in place, which will ensure continuity of service and security of data in the case of an emergency.
- Staff and other users are responsible for the backup and protection of data in accordance with this policy.

ICT Security

Stakeholder CPD has involved cyber security awareness, online safety awareness and GDPR.