Acceptable Use of ICT Policy

Table of Contents

Introduction

To whom does this apply?

This policy applies to:

- All staff members of Redmoor Academy who may have access to a school-owned computers, or mobile devices, regardless of whether or not they use them in their day to day work routine

- All staff/visitors/guests of Redmoor Academy who may be connecting to the school network either via school equipment or their own personal equipment

- All third parties or suppliers who may remotely access any school equipment in the course of their work with the school.

Why is this document necessary?

Redmoor Academy seeks to embrace the use of ICT to enhance teaching, learning and administration within the school.

All organisations (including schools) where computers are in use are required to have a code of practice such as this. It is necessary to outline the principles underpinning appropriate computer use, make expectations clear and ensure users are fully aware of the consequences of not following the code of practice and computer misuse.

This acceptable usage policy has been put together to provide guidance to all users on what is an appropriate use of ICT within Redmoor Academy.

It supplements any legislation around ICT use such as

- Data Protection Act (1998)
- Computer Misuse Act (1990)
- Copyright, Designs and Patent Act (1998)
- Health and Safety (Display Screen Equipment) Regulations 1992 (amended 2002)

- and government guidelines and initiatives such as the Child Exploitation and Online Protection Body (CEOP).

How is this policy communicated and updated?

The ICT Acceptable Use Policy (ICT AUP) is published on the Redmoor Academy website and an electronic version of this document will be shared with all new staff when they join the school as part of the induction process.

Each member of staff is required to complete a Google form confirming that they have read and understood the terms and conditions of the ICT AUP Policy. This will be submitted to the ICT Manager who will maintain a record log. In signing, they accept that they agree to all amendments, which will be published on the school's website unless the ICT department is notified in writing by the individual.

When the ICT AUP is updated a new version will be provided to all staff electronically and published on the website.

Any comments or suggestions for amendments to the policy should be advised to the ICT Manager.

- Visitors, guests and suppliers must be advised of the ICT AUP when attending the school.

- Paper copies are also available from the ICT Manager and Reception for visitors to read.

What are the consequences of improper conduct?

Failure to abide by this AUP, will be treated in the same way as any other misconduct issue and ultimately, could result in dismissal.
Illegal activities will be reported to the police and if necessary the Local Safeguarding Children's Authority.

General Computer and Mobile Device Use

In general, use of ICT equipment (such as computers, mobile devices, printers, faxes), email and the internet within the school should be primarily to enhance teaching and learning or for administrative use.

It is understood however that users may occasionally need to use ICT for personal reasons. This is permitted, as long as such use does not interfere with or lessen their work in school and does not conflict with other aspects of this code of practice.

Priority for computer usage should always be given to the core functions of the school.

Use for business purposes not related to school activities or personal gain is not permitted.

User Accounts:

User accounts are the responsibility of the user.

Passwords must be kept secure and changed when it is deemed necessary.

Passwords must not be written down or disclosed to anyone.

Users must not allow anyone else to use their account nor should they use anyone else's account.

Users must **log off or lock their account when away from their machine.** Accounts are not to be left logged in and unattended.

Some areas may have a requirement for a generic user account, which can be used by a number of individuals, although this is not recommended.

Use of a generic user account must be controlled by one named individual, who is responsible for controlling access to that account, ensuring the password is changed regularly and has a clear understanding of who is using the account, when and for what purpose.

In the case of long term absence or instances where it is deemed necessary or appropriate, school managers may need to access files kept on your hard drive, your Google Drive or your email accounts.

Hardware and Software:

All users are responsible for the care and safe-keeping of any ICT equipment.

Portable equipment such as laptops, iPads (or other mobile devices) must be kept securely when not in use.

Students are not allowed to use USB/Flash drives or other portable storage devices to connect to the hardware owned by Redmoor Academy. This decision has been taken following the increased use of Malware to attack schools.

Staff members are permitted to use external backup storage facilities, such as portable hard drive drives, at the discretion of the ICT Manager, providing that they advise the ICT department of this and that the device is encrypted and protected. (See Appendix C for External Device Use Request Form).

Keep all liquids and food away from any ICT equipment and be aware of the health and safety hazards relating to electrical equipment.

Software is licensed and should only be installed with the authority of the ICT Manager and only on the machines for which it has been purchased.

Users are not permitted to download and install software packages without the authority of ICT.

To comply with the copyright, Designs and Patents Act 1988:

- Users are not permitted to install unlicensed software on any machine
- Users are not permitted to copy licensed software for installation on other machines (school or non-school equipment).

Users should report all faults to ICT (via the ICT helpdesk) as soon as they are identified and not attempt to repair ICT equipment themselves.

Old/broken equipment to be disposed of must be done through ICT as disposal of electrical equipment is now subject to UK government regulations.

Filming, Streaming, Photographing

Staff should not film, stream or photograph individuals or groups of children unless it is related to teaching and learning or development of the school business. Staff should be aware of any students who cannot be filmed or photographed. Staff should use school devices to photograph/film students and should not use their own personal devices for such activities. Staff should not undertake to live stream school footage to social media sites - unless linked to school business and express permission has been granted.

Data

Data must be kept in accordance with the Data Protection Act (see Appendix A).
Do not disclose any information to a third party that could be considered sensitive information.
Do not risk accidental disclosure.
When leaving your computer or device unattended, ensure it is locked or logged out.
Keep your password secure and change it regularly, (at least once a month).
Do not leave your password written down or disclose it to anyone.
Do not allow anyone else to use your account and do not use anyone else's account.
If necessary protect sensitive data with passwords.
Don't forget data stored on other devices such as CDs, DVDs, data sticks and external hard drives is also at risk and subject to the Data Protection Act. All data should be password protected if required.

Users are responsible for the day to day management of their data, being aware of the data storage limits and ensuring unwanted material is deleted on a regular basis.

Internet Usage:

All use of the internet within the school should be primarily to enhance teaching and learning, or for administrative use.

It is understood however that users may occasionally need to use the internet for personal reasons but this should not be at the expense of work.

Use of the internet within the school for the conducting of private business or personal gain is not permitted.

Staff are not permitted to use the internet for any illegal activity; although not specifically against the law this includes accessing sites meant for adults of 18 years or older such as pornographic and gambling websites.

Staff must not search for, or browse through, any sites that contain offensive, obscene, violent, dangerous or inflammatory material.

The downloading of any unlicensed material such as music, video, TV programmes, games, PDF files is illegal and therefore not permitted.

Email

All users are provided with an @redmooracademy.org email account.

This email is accessible from within Redmoor Academy via the staff network and via the internet using the school website.

Be aware that email is treated as data and therefore, is subject to guidelines of the Data Protection Act.

If email is being accessed from a personal or public use computer:

- Do not store anything on the computer hard drive;
- If accessing in a public place, be careful who can see what you are doing;
- Make sure you log off completely.

Email should be treated as inherently <u>insecure</u>.

As with any form of correspondence, be mindful of the language used.

Do not open or forward any email or attachment from an unrecognised source, or that you suspect may contain inappropriate material or viruses.

Do not respond to emails that request personal details, unless you are confident the source is genuine. In general, companies will not request personal data via email. Staff should not provide personal contact details to students. Staff should only make contact with students for professional reasons, using their designated school email address.

Users must not send, forward, print or transmit in any form any offensive, obscene, violent, dangerous or inflammatory material via email.

Users are not permitted to send or forward chain letter emails, jokes, spam etc.

If you are concerned about any email that you may have received, contact ICT (via the ICT helpdesk).

Out of office responses should be used with care. If the response is to be sent outside of the school, be cautious about including personal information such as holiday dates and contact numbers.

Email and Internet Filtering and Monitoring

The school has in place a sophisticated filtering & monitoring system which checks for viruses and traps, suspicious emails. The filtering system denies access to the most undesirable and inappropriate sites on the Internet and maintains a list of banned sites, which is updated on a regular basis.

Whilst this provides a measure of reassurance, it must be understood that the filter does not trap or block everything. Please advise the ICT Manager of any instance where this has occurred, so that it can be blocked/filtered.

Please be aware that:

- Internet access within the school can and will be monitored for inappropriate use;
- All internet sites accessed by users are logged with date and time of access;
- Misuse of the internet and/or email will always result in an investigation as detailed under the school disciplinary procedures.

The accessing and use of inappropriate and indecent materials from the internet or via e-mail will result in disciplinary action being taken which could lead to dismissal.

Social Networking Sites

Staff are **not** permitted to have school students as contacts on social networking sites and are advised to be cautious when allowing contact with other minors (those under 18 years of age), in case of a second or third level connection to a school student. Staff are reminded that ex-students may have friends who are still at the school.

Privacy settings for personal profiles, (and any groups joined) should be used. Never use a personal profile site for a school project, but create a new user profile for this.

Hacking

The Computer Misuse Act 1990 makes it illegal to:

- Gain unauthorised access to a computer's software or data (hacking), including the illegal copying of programs;
- Gain unauthorised access to a computer's data for blackmail purposes;
- Gain unauthorised access to a computer's data with the intention of altering or deleting it, including planting viruses;
- Copy programs illegally (software piracy).

Any type of hacking (defined as an attempt to gain access to folders, databases, or other material on the network to which one is not entitled), is considered to be an extremely serious offence.

To comply with the Computer Misuse Act 1990, any user who indulges in hacking, or is found with hacking software/paraphernalia on their computer or network account, is liable to be dismissed.

Likewise, physical interference with another user's computer or school-owned computer will not be tolerated.

Cyber Attacks

The school has a Cyber-attacks procedure in place, should we experience an attack the ICT manager would implement the procedure, depending on the severity of the attack the school may need to invoke the Business Continuity Plan (see appendix B).

Use of personal devices

Redmoor Academy recognises that many staff choose to access school information from their own devices. Staff may choose to remove physical documents containing personal data from the school setting to enable them to carry out work-related tasks.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, which is above and beyond a simple password protection. Staff must have up to date anti-virus software running on any device that accesses personal data. Staff must ensure that personal devices such as mobile smartphones, tablets and other portable electronic equipment are set to lock and only open with encrypted passcodes to prevent unauthorised access. Any unlawful access of data on such a device will be the responsibility of the owner. Staff must report the loss or theft of devices to the Business Manager and or Principal as soon as is practicable. When exchanging, gifting, upgrading or selling the device staff must ensure that access to any school data is removed and securely deleted.

The school will support and enable staff to ensure that their devices are compliant. Encryption protection will be available for staff and suitable advice provided.

All staff removing documents containing personal information from the school site are responsible for the physical security of the documents whilst in their possession, meaning that they should be stored using the appropriate security measures to comply with UK GDPR. The loss or theft of such documents must be reported to the Business Manager and the Data Protection Officer as soon as is practicable.

If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.

Appendix A: Legislation and Regulations

Data Protection Act (2018):

Anyone who processes personal information must comply with the UK GDPR principles:

- Lawfulness, fairness and transparency
- Purpose Limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and Confidentiality
- Accountability

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Computer Misuse Act (1990):

States that the following actions are illegal

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer material.

Copyright (Computer Software) Amendment Act (1985) and The Copyright (Computer Programs) Regulations 1992:

These acts amended the Copyright, Designs and Patent Act to cover computer software and computer programs making it illegal to:

- Copy software
- Use illegally copied software (pirated copies)
- Electronically transmit software to another location effectively creating a copy.

Appendix B: Cyber Attack Procedure

https://drive.google.com/file/d/1aA-9FHgSV2tTm1LSgMZ3Z5Zsm2BJBm_D/view?usp=sharing

Appendix C: Google Forms

Agreement to terms and conditions - Google Form

https://docs.google.com/forms/d/e/1FAIpQLSck6TI443WdjTuBI3Q5OSpF3CJfkFweblDEDoJ_B3BfKBH2oA/viewform?vc=0&c=0&w=1&flr=0

External Device Use Request - Google Form

https://docs.google.com/forms/d/e/1FAIpQLSdIbedVuMYeOWOLzdDkK7Et7oEhidisKfAbhAkdJ-IpkIB2YQ/viewform?usp=sf_link