Woodsetton School

IT and Acceptable Use policy

Approved by: K Hermon	**Date:** September 2025
Last reviewed on:	September 2025
Next review due by:	September 2026

Staff ICT Acceptable Use policy

Information and Communication Technology (ICT) is an integral aspect of educational effectiveness, professional collaboration, and daily administration within our school environment. As trusted staff members of the school's and academies' technological resources, staff members are expected to set a positive example for students and colleagues in all aspects of ICT usage. This policy outlines the expectations, responsibilities, and obligations of staff when accessing, utilising, and managing ICT systems

Objectives of the Policy

- To promote safe and responsible use of ICT among all users.
- To protect users from harm and safeguard the school's digital assets.
- To support teaching, learning, and administration through effective use of technology.
- To ensure compliance with legal and ethical standards, including data protection laws.
- To encourage digital literacy and citizenship.

This policy applies to all adult users of the schools' systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should complete the School Safeguarding Record Form and retain a copy of the policy for your own records.

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, the Ascent Academy Trust, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

Professional Use and Conduct

- All staff must use ICT resources provided by the school for professional, instructional, and administrative purposes that align with the school's mission and values.
- Staff are responsible for ensuring that their use of digital devices, applications, and the internet upholds the highest standards of integrity, respect, and confidentiality.
- Personal use of school ICT resources should be limited, reasonable, and must not interfere with professional obligations or the safety and security of the school network.

Appropriate Use and Digital Citizenship

Staff are expected to model exemplary digital behaviour, promoting respect, inclusion, and constructive communication in all online environments.

Use of ICT resources for purposes that are illegal, discriminatory, harassing, or in violation of school policy is strictly prohibited.

Staff should proactively guide students on safe and responsible use of technology, digital etiquette, and the identification of potential online risks.

Acceptable Use of ICT Resources

- ICT resources must be used in accordance with the school's ethos and educational goals. Acceptable use includes, but is not limited to:
- Accessing and sharing educational materials as directed by teachers or staff.
- Researching academic topics using credible sources.
- Communicating respectfully with peers, staff, and external collaborators.
- Completing assignments, projects, and assessments using approved platforms.
- Participating in virtual classes, forums, or extracurricular groups hosted by the school.
- Utilising school email and messaging services for appropriate educational purposes.

Unacceptable Use

- Actions that constitute unacceptable use include:
- Accessing, creating, or sharing inappropriate, obscene, or offensive content.
- Use of ICT resources for bullying, harassment, or intimidation.
- Attempting to bypass security measures or accessing restricted files or accounts.
- Engaging in illegal activities, including copyright infringement, hacking, or fraud.
- Installing unauthorised software or hardware or altering system configurations.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences. In line with this policy, the following statements apply:-
- If you download any image, text or material check if it is copyright protected. If it is, then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally, report it to a senior member of staff.
- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.

- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.

You should not:

- introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- seek to gain access to restricted areas of the network;
- knowingly seek to access data which you are not authorised to view;
- introduce any form of computer viruses;
- carry out other hacking activities

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

- providing evidence of business transactions;
- making sure the School's business procedures are adhered to;
- training and monitoring standards of service;
- preventing or detecting unauthorised use of the communications systems or criminal activities;
- maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Head teacher.

- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored. School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group. Social networking applications include but are not limited to:
- Blogs • Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flickr
- 'Microblogging' applications e.g. Twitter

When using school approved social networking sites the following statements apply:-

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for pupils to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @woodsetton.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries.
- Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Security and Data Protection

- Staff must safeguard access credentials, avoid sharing passwords, and report any suspected breaches immediately to the appropriate ICT personnel.
- Confidential information regarding students, colleagues, or the institution must not be disclosed or transmitted without proper authorisation.

- All digital records, communications, and educational materials must be managed in accordance with school policy and applicable data protection legislation.

The processing of personal data is governed by the Data Protection Act 1998 and Digital Personal Data Protection Act 2023.

Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School's premises or working remotely you must:-

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions; familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

Maintenance and Reporting

- Staff are responsible for the proper care and maintenance of any devices assigned to them, including timely updates and adherence to security protocols.
- Any malfunctions, security incidents, or suspected misuse of ICT resources must be reported promptly to the ICT support team.

Continuous Improvement

- Staff members are encouraged to participate in professional development related to ICT, staying current with new technologies and best practices.
- Suggestions for enhancing ICT policies, infrastructure, or digital learning opportunities are welcome and should be directed to school leadership. By adhering to these guidelines, staff reinforce a culture of safety, responsibility, and innovation.