

ETTINGTON C of E PRIMARY SCHOOL

Reviewed November 2024



Learning for Fullness of Life
Trust-Respect - Love

STAFF ACCEPTABLE USE POLICY

Date of publication: November 2024

Review date: November 2025

TERMS OF REFERENCE

The internet and e-mail play an essential role in the conduct of our business in school. The systems within our school are made available to children, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There is substantial investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively. How we communicate with people not only reflects on us as individuals but on the school. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of email and the internet. 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. For your safety, we are able to monitor all web pages visited, email sent and received. This helps us monitor inappropriate use, such as bullying. This policy applies to you as an employee whatever your position, whether you are a headteacher, teacher, support staff, permanent, temporary, or otherwise. Any inappropriate use of the school's internet and email 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. It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Headteacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Headteacher.

GENERAL PRINCIPLES AND LEGAL ISSUES

All information relating to our pupils, parents and staff is confidential. You must treat all school information with the utmost care whether held on paper or electronically. Care must be taken when using email as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements. We trust you to use the internet sensibly. Please 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. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information. However, the same principles apply to information exchanged electronically in this way as apply to any other means of communication. For example, 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.

Internet and email 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 Headteacher. 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 where it is necessary for your duties. The processing of personal data is governed by the General Data Protection Regulation. Schools are defined in law as separate legal entities for the purposes of complying with GDPR. Therefore, it is the responsibility of the school, and not the Local Authority, to ensure that compliance is achieved. 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.

MONITORING COMMUNICATIONS

This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

- To establish the existence of facts.
- To ascertain compliance with applicable regulatory or self-regulatory practices or procedures.
- To ascertain or demonstrate effective system operation technically and by users.
- For national security/crime prevention or detection.
- For confidential counselling/support services.
- For Investigating or detecting unauthorized use of the system.
- For monitoring communications for the purpose of determining whether they are communications relevant to the business.

Warwickshire LA has an obligation to monitor the use of the internet and email services provided as part of the Warwickshire Broadband service to schools, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. Warwickshire LA 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 send and receive electronic communications.

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.

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.

INTERNET USE

When entering an internet site, always read and comply with the terms and conditions governing its use. Do not download any images, text or material which is copyright protected without the appropriate authorisation. Do not download any images, text or material which is inappropriate or likely to cause offence. If you want to download any software, first seek permission from the Headteacher and/or member of staff responsible. They should check that the source is safe and appropriately licensed.

You are expressly prohibited from:

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

For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- Unauthorized access to computer material i.e. hacking.
- Unauthorized modification of computer material.
- Unauthorized access with intent to commit/facilitate the commission of further offences.

USE OF EMAIL

You should agree with recipients that the use of email is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted email 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. It is good practice to re-read email before sending them as external email cannot be retrieved once they have been sent.

DATA PROTECTION

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 Headteacher or line manager.
- Familiarise yourself with the provisions of the General Data Protection Regulation (GDPR) 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. The school may view any GDPR breach

misconduct or gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.