

To ensure that all employees are responsible for the safe use of ICT, the following guidelines have been established. No policy can lay down rules to cover every possible situation. Instead, it is designed to express the philosophy of the school and set forth general principles when using electronic media and services.

1. PROHIBITED COMMUNICATIONS

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing
2. Derogatory to any individual or group
3. Obscene, sexually explicit or pornographic
4. Defamatory or threatening
5. In violation of any license governing the use of software
6. Engaged in for any purpose that is illegal or contrary to the school policy or interests

2. PERSONAL USE

The computers, electronic media and services provided by the school are primarily for educational use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

3. ACCESS TO EMPLOYEE COMMUNICATIONS

Generally, electronic information created and/or communicated by an employee using email, word processing, spreadsheets, Internet and bulletin board system access, and similar electronic media is not reviewed by the school. However, the following conditions should be noted:

1. The school does routinely gather logs for most electronic activities or monitor employee communications directly, for detecting patterns of use that indicate employees are violating school policies or engaging in illegal activity.
2. The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies. The schools email system will modify all messages by adding a disclaimer to the footer of all outgoing emails.
3. Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means. Under no circumstances should pupil named data be transmitted over the Internet or email. The school office has use of encrypted data systems for this purpose.

4. SOFTWARE

To prevent breach of licensing regulations, only software registered through the school may be installed onto school owned equipment. Before downloading or installing any software you must gain permission from the Network Manager.

5. SECURITY

Staff have a responsibility to maintain the security of the schools electronic systems and should:

1. Ensure laptops are physically secure by using the laptop lock provided at all times
2. Report any loss or damage to equipment immediately
3. Not divulged their login details to anyone and not log anyone else on as them
4. Never leave their computer unattended whilst logged in – always lock your computer
5. Always logout and shutdown at the end of each day

6. Not allow pupils to use designated admin machines, as they could gain access to privileged information and contravene the Data Protection Act

6. VIRUSES

Antivirus software is installed on all School owned machines. This software is updated daily to ensure the latest viruses cannot affect the schools network. It is the responsibility of all staff to ensure they virus check any removable media, such as floppy disks, CD's and USB memory sticks before use.

7. APPROPRIATE USE

Employees must respect the confidentiality of other individuals electronic communications. Except in cases in which explicit authorisation has been granted by school management, employees are prohibited from engaging in, or attempting to engage in:

1. Monitoring or intercepting the files or electronic communications of other employees or third parties.
2. Hacking or obtaining access to systems or accounts they are not authorised to use.
3. Breaching, testing, or monitoring computer or network security measures.
4. No email or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.
5. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
6. Anyone obtaining electronic access to other companies or individuals materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

8. PARTICIPATION IN ONLINE FORUMS

The school recognises that participation in some online forums, Internet mailing lists, bulletin boards etc... might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area. But employees should remember that messages sent on school provided facilities to one or more individuals via an electronic network are statements identifiable and attributable to the school.

9. VIOLATIONS, SANCTIONS & REPORTING OF ACCIDENTAL VIOLATIONS

In the event of an accidental violation, for example accessing an inappropriate website in error, you must contact the Network Manager immediately.

10. EMPLOYEE ACCEPTANCE

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of Cromwell Community College's computers, networks and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that violations of this guideline on appropriate use of the email and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability.

I further understand that my use of email and the Internet may reflect on the image of Cromwell Community College to our pupils, parents, governors and suppliers and that I have responsibility to maintain a positive representation of the school. Furthermore, I understand that this policy can be amended at any time.

Signed: _____

Print: _____

Date: _____