



ICT AND INTERNET USAGE POLICY – PUPILS

The IT Manager is responsible for the formulation and review of policies affecting the use of computers within the School. These policies include co-operation with outside bodies such as the Data Protection Registrar, the Health and Safety Executive and the British Computer Society to ensure that the policies reflect current best practice and comply with any laws or regulations controlling the use of computers. These policy documents are subject to review by the Senior Leadership Team but ultimate responsibility for their content rests with the Headmaster and the Finance Director.

All students are required to comply with these policies when using computers owned by the School or other computers when used for work on behalf of the school or on school premises.

General Rules

The general rules are posted in every computer room and are subject to alteration as circumstances dictate. In general, everyone is expected to use the facilities provided in a reasonable and responsible manner and behave in such a way as to permit everyone to work to their best advantage.

Health & Safety

The hazards associated with computing are relatively minor and are assessed by the IT Manager.

Confidentiality

Every effort is made to protect the security and confidentiality of pupils' work on the networks. This has to be balanced against the School's responsibility to maintain internal rules and regulations and to comply with any relevant laws.

Copyright

The ownership of work produced by pupils can sometimes be in doubt. The School's policy is to interpret the law as generously as possible in favour of the author while retaining the rights only to such items as are covered specifically by this policy.

Computer Misuse Act

The unauthorised use of computers is a criminal offence. The Computer Misuse Act of 1990 formalises this and explains the different offences and penalties.

Acceptable Usage Policy

This policy applies to all pupils who use the School's IT facilities and sets down the standards which pupils are required to observe in the use of the IT network, email and the internet.

It is the responsibility of all pupils to acquaint themselves and comply with this policy. Certain terms in this policy should be understood expansively to include related concepts:

School includes all Framlingham College locations and both academic and non-academic areas.

Document covers any kind of file that can be read on a computer screen as if it were a printed page, including the HTML files read in an internet browser, any file meant to be accessed by a word processing or desk-top publishing programme or its viewer or any other electronic publishing tools.

Graphics includes photographs, pictures, animations, movies or drawings.

Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

The acceptable usage policy is split into four sections:

- Internet
- Email
- Security
- Copyright

BY LOGGING ON TO THE FRAMLINGHAM COLLEGE NETWORK YOU SIGNIFY YOUR ACCEPTANCE OF THIS POLICY, AND YOU SHOULD SEEK CLARIFICATION OF ANY ISSUES THAT YOU DO NOT UNDERSTAND.

Internet

Use of the Internet by all pupils is permitted and encouraged where such use is suitable for school purposes and supports Framlingham College's aims. In addition, at specified times and locations, pupils may access the facilities for personal activities including communication and recreational use.

Personal use should never compromise availability for academic use.

The Internet is to be used in a manner which is consistent with Framlingham College's standards of professional business conduct and as part of a pupil's academic research.

The use of a VPN is not permitted to attempt to bypass the school filters to access content that is not permitted.

During School hours we expect you to use your Internet access for School related purposes only to research relevant topics and obtain useful School related information.

Access to the Internet is available in various locations around school and on personal devices until various times depending on year group. This is to be used for genuine research purposes and School related enquiries during school hours.

All existing School policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of School resources, sexual harassment, fraud and information security and cyberbullying.

Where possible, pupils should schedule resource-intensive operations, for example, large file transfers, video downloads and mass emailing for off-peak times.

Any file, including emails, that is uploaded or downloaded must be scanned for viruses before it is run or accessed. This should be done automatically, so pupils must check that their anti-virus software is running. Contact the IT department for advice if you are unsure how to do this.

Pupils should be particularly careful not to disclose any personal or identifying details when using newsgroups or chat-rooms. Avoid the use of names, telephone numbers and locations. Under no circumstances should personal or School addresses be given out.

The School's Internet facilities and computing resources must not be used knowingly to break the law. Use of any School resources for illegal activity is grounds for immediate discipline and the School will co-operate with any legitimate law enforcement agency.

Any legal and licensed software or files downloaded via the Internet into the School network become the property of Framlingham College. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

- No pupil may use School facilities knowingly to download or distribute pirated (illegal and unlicensed) software or data.
- No pupil may use the School's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the security of another pupil.
- No pupil may use the School's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door programme code.

Pupils are specifically prohibited from downloading any software without the express permission of the IT department.

Pupils with Internet access may not upload any software licensed to the School or data owned or licensed by the School without explicit authorisation from the member of staff responsible for the software or data.

The School's monitoring system (Lightspeed) records (for each and every pupil) each web site visit, each chat-room, newsgroup or email message and each file transfer into and out of its internal networks. No pupil should have any expectation of privacy as to his or her Internet usage. The IT department will review internet activity and analyse usage patterns, and may choose to publicise this information to ensure that School internet resources are devoted to maintaining the highest levels of productivity.

Pupils should not download or view material that is obviously libelous (or otherwise unlawful), or inappropriate in any way, i.e. graphic images, sound files or music.

Framlingham College reserves the right to inspect any and all files stored on School computing facilities in order to assure compliance with this policy.

It is acknowledged that certain pupils may require, during the normal course of their studies, access to certain sites that may normally be blocked. It is possible to make exceptions in these cases to allow legitimate access by contacting the IT department; please note that a member of staff may be required to confirm your requirements before access is granted.

The category restrictions relating to Internet access are extended before and after working hours. For example, access to Hotmail, Yahoo and Facebook is allowed.

Access to Social Networking sites is only permitted outside normal School Hours.

The School has in place a firewall to ensure the safety and security of the School's networks. Additional devices may also be installed in the future to further protect these networks. Any pupil who attempts to disable, defeat or circumvent any School security facility will be subject to immediate disciplinary proceedings.

A PUPIL WILL BE HELD ACCOUNTABLE FOR ANY BREACHES OF SECURITY OR CONFIDENTIALITY

Email

Pupils need to be aware that e-mail carries exactly the same status as other forms of communication, including letters, memos and telephone conversations, and the same consideration and legal implications need to be applied and observed in the use of email as in these other forms of communication.

The School provides an online e-mail system, via Microsoft Office 365, to support its academic and administrative activities and access to e-mail facilities for all users is granted on this basis. Pupils are reminded that e-mail sent and received on the School's systems are not private property they remain part of the School's information systems. Personal use should never compromise availability for academic use.

When composing and sending an e-mail, it is expected that the content meets the standards of professionalism which Framlingham College expects of its pupils.

It is not permitted for pupils to send sexual, racially biased or other inappropriate emails, which would infringe the School's code of conduct. Do not use aggressive, abusive or deliberately anti-social language. Never email hastily or out of anger.

Use of personal email must not detrimentally affect the duties of other pupils or disrupt the system, and/or harm the School's image or reputation.

Pupils should not copy, download or forward material that is obviously libelous (or otherwise unlawful), unrelated to work, or inappropriate in any way, i.e. graphic images, sound files, or music.

Access to Internet or web-based email (i.e. Hotmail or Yahoo mail) is permitted for pupils only outside of normal school hours. Be aware that this mail is insecure and may present a security threat.

Pupils are reminded that they are responsible for their own email housekeeping. Unwanted email should be deleted. If pupils are unsure how to achieve this, guidelines are available from the IT department.

Pupils should not give their external email address out carelessly. Only enter it on business circulars and application forms if you are sure that it will not be misused or forwarded on.

Particular attention should be paid to the addressee to ensure the message will reach the intended recipient especially if choosing from an address list of similar names.

Messages intended for another recipient should be re-directed and then deleted. Any incorrectly addressed messages should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

Security

Pupils should not allow other pupils to use their network login. Do not leave your PC logged on to the network.

Anti-virus software is installed on every PC connected to the School's network. Anti-virus software must not be disabled or uninstalled for any reason. The anti-virus software is set up to regularly scan each PC for viruses. If pupils notice that their anti-virus software is not running or scanning, they should immediately report the fact to the IT Department.

It is extremely common for a virus to propagate itself via an e-mail attachment. The attachment may be in various forms, but commonly PDF, TXT, EXE, ZIP etc. There may also be a link within the body of an email encouraging you to click. You may also receive a phishing email, which is an attempt to trick you into sharing your login details or bank/credit card information. Many of these emails have been designed with great effort to look authentic from a genuine organization. If there is any doubt as to the authenticity of an e-mail, it must not be opened and reported to the IT department immediately.

It is also common for a virus to use the Outlook address book to forward itself to others. This means that infected email could be received from a known and trusted source. Pupils should be immediately suspicious if the email is unusual in any way.

Framlingham College maintains the right and ability at any time and without prior notice, where justified, to inspect any information stored on any device that accesses the School network in order to ensure compliance with the policy.

If clarification of any aspects of policy are required, refer to your Housemaster/Housemistress, Tutor or the IT department.

Copyright

Every piece of work created belongs to someone. This includes text, images and any other form of intellectual creation regardless of how and where it is stored.

The majority of the software used within the School is owned by or licensed to Framlingham College and is protected by various patents, copyright and license laws currently in force.

The copyright ownership of all material must be respected and the wishes of the copyright owner are to be observed.

No material may be copied from the Internet or any other electronic source save with the specific permission of the copyright owner. Stringent laws apply, in particular, to the scanning of material. The use of all such material is to be properly attributed.

No-one is permitted to make copies of or changes to any software owned by or licensed to Framlingham College except where specific permission has been granted so to do. This includes any upgrades, 'plug-ins' or new versions regardless of the source.

The copyright of any material that is commissioned by Framlingham College, produced as coursework or for which remuneration or other consideration has been given by the School, is the property of Framlingham College.

Scanning or digital manipulation of documents, diagrams, photographs etc. that are copyright may be done only with the express permission of the copyright holder and in accordance with current law.