



PUPIL ICT ACCEPTABLE USE POLICY

Overview

This policy covers the use of ICT within St Margaret's School for Girls, and is intended to cover most aspects of the use of modern technologies. It is expected that all users will read and follow these as part of being a responsible member of the St Margaret's community and in line with the ethos of the school. We interpret the term 'ICT' to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically.

This policy covers pupils' use of ICT, AV and digital equipment provided by the school and also digital equipment brought into school by members of the school community (such as cameras, mobile phones or other electronic devices).

The ICT facilities are provided for the purposes of educational research, learning and to support the operational business of the school. The use of the technology is a privilege, not a right and access to the system is provided in an ethos of trust. Similarly, any pupil should use the internet (including social media) with respect, regardless of whether they are accessing sites at school, at home or elsewhere. The school will treat as a disciplinary matter any instance of ICT misuse that brings the school or members of its community into disrepute.

We expect all users to use the technology in conjunction with the laws relating to data protection, computer misuse and offensive materials acts.

This policy covers:

- Security of passwords
- E-mail etiquette, including language to be used
- The use of the Internet, including site access
- Respect of copyright
- Economic use of equipment and printing
- Correct use of equipment
- Mobile devices including phones, iPods and media players

Use of the technology may be withdrawn from any user operating outwith the code outlined in this agreement.

All users should be aware that the online activity through school resources of every individual is recorded and monitored. If foul play is suspected, a user's activity can then be tracked back to the individual. E-mail is the legal responsibility of the school and is filtered by several electronic systems. If it is suspected that an individual is misusing the ICT network and/or online provision, then the Head reserves the right to access their network share and e-mail.

General Use of School Equipment

The ICT network and associated hardware is developed and looked after by the Network Manager who is responsible for the following:

- Maintenance of equipment
- Moving equipment
- Installing software
- Virus protection
- Setting up and installation of equipment

These duties above are specific to the Network Manager and should not be carried out by anyone else.

No one should:

- Tamper with hardware
- Disconnect any cable or additional item from any piece of school equipment
- Connect or add any piece of equipment to that which belongs to the school. (ie ipods)
- Download and install software
- Install software from any other device
- Plug in and tamper with the network to cause disruption to the service provider

Whilst sitting at a computer or using another piece of school equipment users must:

- Ensure they are sitting correctly
- Follow health and safety advice on the equipment
- Take a break for every hour of use and avoid looking at a screen for more than an hour at a time
- Have suitable lighting to view a screen without reflection or dazzle

In order to keep the equipment clean, users must not:

- Eat or drink whilst using a piece of school equipment. This will help to avoid sticky keys on keyboards

ICT Support

The Network Manager provides support for all school users.

Software Installation

Pupils are not permitted to install software on the school network. A licence is required for every piece of software installed. Software can only be installed by the Network Manager.

Fault Reporting

Faults should be reported to a member of staff who will then complete an online fault report form on the school intranet page. This provides the most efficient method of responding to and tracking faults/issues for the Network Manager.

File Management

The school requires all users to ensure that their storage areas are kept up-to-date and, if files are no longer required, they are either to be deleted or burnt to a DVD/CD and then deleted on the system.

Every user is provided with a personal area in which to store work. Videos and audio files should be stored in the Media Folder. (The storage of personal photographs and/or video is not permitted.)

The storage and/or distribution of illegal or copyright materials is not permitted. If anyone discovers that another user is storing or distributing illegal materials, then this should be reported to the Senior Leadership Team immediately.

E-mail

Every e-mail communication from the school is the legal responsibility of the school. As an organisation we must apply the following conditions on the use of e-mail communications:

School e-mail will be filtered for the use of unsuitable language both on receipt and on the sending of mail.

All mail received into the school is verified against a variety of electronic tests which validate authenticity and try to remove SPAM and other unsuitable communications.

All mail is stored and recorded in the mail archive server.

The mail account is for educational use and responsible personal use. Users must not do any of the following:

- Use swear words or other profanity, including those structured to try and deceive the filters with spaces and/or * etc.
- Pass on jokes, chain mail, junk mail, spam, hoax viruses or their warnings.

Mailing Lists

Subscribers to mailing lists must unsubscribe and clear their accounts before leaving the school.

Spamming

SPAM emails should be deleted immediately. SPAM is created to cause disruption to mail systems by overloading the mail system thus slowing it down or stopping it completely. If there is any doubt about whether an e-mail is SPAM, the Network Manager will advise.

Web and other online usage provision

The internet access supplied by the school is primarily to support the educational work of students and staff and the business function of the school. The personal use of the school's internet access should not cause any disruption to the school's access and may not be used to support an individual's private business or enterprise. The school reserves the right to block or remove an individual's internet access at any time.

All internet activity in the school is logged. These logs can be checked at the request of the Head. The school provision of internet access is fully filtered. This may prevent access to a page that is required. If this is the case a request can be made by a member of staff. Any unsuitable web page should be brought to the attention of the Network Manager. The deliberate act of trying to bypass the filtering and protection placed on the network by any user will be referred to the Head.

Downloading

Pupils are permitted to download reference material to support their studies. The copyright on all material must be observed. If information from the internet is used, this must be referenced correctly in a bibliography. Pupils are not permitted to download and store or stream copyrighted material across the internet.

In general pupils are not permitted access to YouTube nor any other site that has the potential to distribute content that is not appropriate or suitable. However, VS and VIS pupils may have access to streaming media in relation to their studies.

Offensive Material

Users are not permitted to download, show or distribute offensive materials. Misuse will be referred to the Head and action will be taken at the discretion of the Head.

Antivirus

The school runs a comprehensive antivirus system. The antivirus software is updated automatically when the latest profile is received.

Messaging / Chat / social networking sites / Anonymizer sites

These are prohibited on the school network apart from those available inside the mail system and other authorised systems.

Security

Users of the school network are provided with a username and password. A user's password is private. All users must take responsibility for their actions on the school network. Any misuse of the school network will be referred to the Head.

No one should access another user's account. No user should leave a PC when he or she is logged on. Users will be asked to change passwords on a regular basis.

Make sure you log off when you are finished!

Mobile Technologies in Junior School

For some of our older junior girls, mobile phones are a useful means of communication between the girls and their parents at the end of the school day. However, during the day, if girls need to contact home they should go to the school office where one of the office staff will contact home for them. Girls should not use their mobile phones for these calls and, whilst at school, phones, must never be used for taking photographs, playing games or text messaging friends. If it is necessary for a junior pupil to have a mobile phone at school, the phone must be switched off and stored in her school bag during the day. These phones are brought into school at your own risk.

Mobile Technologies in Senior School

(see 'Use of mobile phones in Senior School policy')

Senior school pupils and staff are permitted to carry electronic devices in school and on project trips. Individuals are responsible for the safety of their own equipment and the school cannot take responsibility for it. All members of the community must use their devices responsibly and with respect to others. Any misuse may result in confiscation of the device.

All users are reminded that the sending of texts and other call information is stored by their mobile phone service provider. It should be noted that the misuse of technology to abuse others is illegal and individuals who deliberately abuse others may be prosecuted.



ICT ACCEPTABLE USE AGREEMENT - PUPIL

In the context of the School's Acceptable Use for Information and Communication Technologies and other school policies, I will:

- Be responsible for monitoring and appropriately rejecting information accessed or received by me.
- Be courteous and use language which is not obscene, abusive or harassing and will report any such usage against me to a member of staff.
- Accept responsibility for keeping copyrighted material from entering the school; this means that I will not download any software material which is copyrighted, nor post or distribute copyrighted material.
- Only download non-copyright material in an appropriate manner for academic assignments, listing its source in a bibliography and clearly specifying any quoted material.
- Abide by the current sign-on procedures, protect my username and password and **log off after use.**
- Limit my printing to only the items I require and minimise waste.

I will not:

- Misuse a computer or any other associated technology on the school network.
- Permit other people to use my log-on account or e-mail account.
- Create, access or transmit any material that would be considered defamatory, offensive or illegal (i.e. obscene, indecent, racist, violent, inciting extremism etc.)
- Use valuable internet time playing non-educational games.
- Generate or pass on chain letters.
- Reveal personal information (names, addresses, telephone numbers and other details) about myself or others.
- Interfere with the work of others or with the computer systems.
- Use my mobile phone or any other device inappropriately during the school day in line with school policy.
- Photograph/video or distribute photographs/videos of other members of the St Margaret's community without their permission.

I understand that if I violate any of the terms of the ICT Agreement, I may be denied independent access to the technology and may face further disciplinary action. I am aware that each case will be considered on its merits.

Pupil Name

Pupil Signature

Parent Name

Parent Signature

Date