Felpham Community College
ICT Acceptable Use Guidance

As agreed by The Governing Body, the Senior Leadership Team of Felpham Community College adopted the ICT Acceptable Use Guidance for all staff and students on 25 October 2021.

Introduction

ICT resources, including Internet access, are potentially available to all students and staff within the school. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will be considered a disciplinary matter.

The college networked resources are for educational purposes and may only be used for legal activities consistent with the rules of the college.

Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the college or County Council into disrepute is not allowed.

The school expects that students will use ICT appropriately within the curriculum and that staff are responsible for providing guidance and instruction in the use of these resources. Staff need to be vigilant when supervising students using computers, especially when using the internet. Misuse of the computer system by students will be dealt with in accordance with normal school disciplinary procedures.

Use of the network, Internet, Intranet or the college's Microsoft 365 deployment will only be permitted upon receipt of a permission and agreement form signed by the student and a parent or legal guardian.

ICT resources are regularly monitored to ensure they are being correctly used by staff and students.

Conditions of Use

The following conditions of use include all computers in the school, all computers owned by the school which may be used off-site, and all school computer networks.

Personal Responsibility

1. **Access** to the networked resources is a privilege, not a right.
2. Users are responsible for their behaviour and communications made using the school ICT resources.
3. Staff and students must only use the resources for the purposes for which they are made available.
4. Users are to take due care with the physical security of hardware they are using.
5. Users are responsible for reporting any misuse of the network to IT Support.
   Any misuse of the network will be reported to the Leadership Team member responsible for ICT or the Headteacher immediately.
6. Staff and Students will have regular mandated password changes. Two-Factor (Multi-Factor) authentication is required for all staff.
7. Staff should lock their computers when they intend to leave them unattended.

Acceptable Use

Users are expected to utilise the network system in a responsible manner. It is not possible to set definitive rules about acceptable usage, but the following list provides some guidelines:

Network Etiquette and Privacy

Students and staff are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users.
5. Students must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
6. Do not use, or attempt to use, another user's password to gain entry to ICT resources or folders.
7. Password – do not reveal your password to anyone. If you think someone has learned your password then contact IT Support immediately for a password change.
8. Electronic mail – is not guaranteed to be private. **All messages will be monitored against a list of appropriate keywords in order to meet safeguarding requirements.** Messages relating to or in support of illegal activities will be reported to the County Council or police. Do not send anonymous messages.
9. Disruptions – do not use the network in any way that would disrupt use of the network by others.
10. Users will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
11. Students finding unsuitable websites through the school network should report the web address to IT Support.
12. Do not introduce "USB drives" into the network without having checked for viruses. "USB drives" should only contain files to support learning.
13. Do not introduce files into your Microsoft 365 account without having checked for viruses. Office 365 should only contain files to support learning.

14. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity). All network activity is monitored, including devices owned by the college that are taken offsite. All sites visited leave evidence in the network, if not on the computer. Downloading some materials is illegal and the police or other authorities may be called to investigate such use.
15. **Users should not make use of VPN (Virtual Private Network) services in order to bypass the internet filtering which is set by the college, when making use of the BYOD scheme.**
16. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
17. Files held on the college's network or **Microsoft 365** will be regularly checked by the IT Support and should not be deemed as private.
18. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the network does not occur.

Unacceptable Use

Examples of unacceptable use include but are not limited to the following:

1. Students are not allowed to use another student's workspace even if that student gives verbal or written permission.
2. Students finding workstations or laptops logged on under another user's should log off the machine whether they intend to use it or not.
3. Accessing or creating, transmitting, displaying or publishing any material (eg images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The school has filters in place to block e-mails containing language that is or may be deemed to be offensive).
4. Accessing or creating, transmitting or publishing any defamatory material.
5. Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
6. Receiving, sending or publishing material that violates the Data Protection Act or breaching the security this act requires for personal data. Transmitting unsolicited material to other users (including those on other networks).
7. Unauthorised access to data and resources on the college network system or other systems.
8. User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
9. Any breach of the provisions made in UK General Data Protection Regulation 2018 (GDPR)

Additional guidelines

1. Users must comply with the acceptable use policy of any networks that they access.
2. Users must not download software without approval from the ICT team.
3. Users must comply with software licence agreements and copies of licence agreements must be provided to the ICT team prior to software being loaded onto the network.

Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the network or your errors or omissions. Use of any information obtained via the network is at your own risk.

Network Security
Users are expected to inform the IT Support team immediately if a security problem is identified. Do not demonstrate this problem to other users. Users identified as a security risk will be denied access to the network.

Physical Security
All users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away or returned to the ICT department when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

Wilful Damage
Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the college network will result in loss of access, disciplinary actions and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited. The college reserves the right to request re-imbursement by parents / carers in extreme cases.

Media Publications
Named images of students (e.g. photographs, videos, web broadcastings, blogs, TV presentations, web pages etc) will not be published on the internet.

The college uses digital video as a medium to enhance teaching and learning; this material is only to be used for educational purposes. If parental consent has not been given every effort will be made to remove instances in which such students are shown. If large groups are being filmed this may prove impractical.