ICT Acceptable Use Policy

Contents

Acceptable Use of ICT and e-Safety Policy

Intended Audience

The audience for this document includes all teaching and administration staff who will either be using College ICT equipment or College ICT infrastructure either on or off site at any point. This covers Desktop, Laptops and mobile devices such as iPads and e-Safety.

Purpose of Policy Statement

The purpose of this document outlines the expectations that the college has of all users and their responsibility to College information and equipment. It is not exhaustive and it is expected that all readers of this document will use common sense and their initiative with regards to issues not fully detailed within.

Summary Points of the Acceptable Use Policy and e-Safety Policy

By agreeing and signing up to these summary points you are confirming that:

1. You have read and understood all the points detailed in this document
2. You understand what is meant by responsible use and care of ICT equipment within the College
3. You understand that you will look after your user name and password and lock your desktop/laptop PC whenever you leave it unattended
4. You understand the issues around e-Safety and responsible use and activities on the internet
5. If you are issued with a college device such as an IPad or Laptop you will look after it and pay for any repairs/replacements (including cables and chargers) it if it is damaged or lost whilst in your care
6. You understand that all College computers are managed with Forensic Policy Central Software and your web and computer activity may be flagged centrally
7. You are using the College ICT equipment and as such it is for work use rather than personal use.

Print Name

Signed

Date

Full Term and Conditions of the Acceptable Use and e-Safety Policy

Roles and Responsibilities of Staff

Staff are reminded that they are responsible for student use of ICT whenever they use equipment, this includes:

- Supervision of students with ICT
- Reporting any damage found or occurred including logging on SIMS
- Report misuse of ICT to the ICT helpdesk
- Promote good practice with ICT with students at all times

General Use of ICT

Users are expected to take responsibility for use of all ICT making sure that the technology is used safely, responsibly and legally. Users should be aware of the opportunities and risks posed by new technologies and also to make pupils aware of e-safety measures.

College users may only download or install any software or files on school's ICT equipment as agreed with the school's technical/ICT staff. Extra due care and attention is also needed when opening e-mails and attachments from unknown people. Any issues with hardware or software should be reported to the ICT helpdesk.

College users must not intentionally gain access to unsuitable or illegal sites e.g. pornography, child abuse, racism, incitement to violence. Accidental access to such sites should always be reported as soon as possible to the ICT team.

Access to computer systems is only via a users' own login and password, which must be kept secret in the same way a PIN number for a bank card would be. Accessing files that do not belong to a user or they do not have permission to view is classed as hacking and the user will be in violation of the Computer Misuse Act 1990.

Users work should not break The Copyright, Design and Patents law. The source of information (words, images etc.) should always be acknowledged.

The College does not permit storage of illegal music and video files to be kept anywhere on the College network. If you need clarification of the legality of files, please ask the ICT helpdesk.

College ICT equipment should always be used with care and any damage reported as soon as possible to the ICT helpdesk.

Users should lock their computers (CRTL-ALT-DEL and choose lock) whenever they leave their desk to ensure there is no unauthorised access of information.

Responsible use of network resources includes:

- Only printing when necessary
- Regularly reviewing files in your user area and deleting them when no longer needed

- Only storing school-related files and images on the school network
- Only using the ICT equipment for school related work

Use of ICT during personal time

Laptops have been left in the staff room and are available for staff use during break and lunchtimes. Access to sites such as eBay and online shopping sites are permitted during lunch and break times but not throughout the school day. Excessive use of non-teaching and non-educational sites may be flagged with the appropriate member of SLT for further action.

Social Media

Staff accounts on the school network do have access to twitter and Pinterest but users are reminded of the risks when using social media where they may be exposed to content that is not suitable in school. Twitter and other forms of social media use in school time should be restricted to "official" Ellesmere accounts and should reflect the college ethos and aims at all times.

Users should never exchange personal details with students when using social networking sites and must ensure that their personal privacy settings are set at maximum. Users are also remained to consider their "social media footprints" and check security and privacy settings so they are not leaving themselves at risk.

Users are also reminded that appropriate language should be used at all times and that they should conduct themselves professionally at all times.

Computer Monitoring

All College devices have got Forensic software installed and this may capture users' screen shots and words they have typed for the internet or PC itself. Any issues around students are flagged to the SSO's and SLT. Issues around staff will be flagged to SLT directly.

File Back Up

All files on the network are backed up automatically. All network users (including VPN users) should save their work on the network folders they have access to. Members of staff are permitted to make personal backups of files on removable media if they require, however all devices will be scanned by antivirus software before they can be used on the College network.

Requests for files accidently deleted need to go via the helpdesk.

Virus Protection

All computers have ESET antivirus software loaded. This will update automatically and scan from time to time. It is not permitted to disable or remove the ESET software from any college device. If the Antivirus software is not updating or is out of date, support should be sought from the ICT team.

Warranty

All devices are supplied with a minimum one year manufacturer's warranty covering parts and labour. However, warranty usually excludes damage due to:

- Accidents
- Unreasonable use, abuse, neglect and alterations
- Improper service, improper installation, improper connection with peripherals
- Damage to or loss of any programs, data or removal storage media
- Any attempt by members of staff to dismantle or repair their laptops or install modifications themselves will invalidate the manufacturer's warranty

Repairs required for any of the reasons above should be reported through the college's help desk and carried out by a member of the ICT team. Damage to College equipment in the care of staff will result in the responsible staff member paying for repair or replacement units.

Technical Support

Users should not attempt to repair any hardware faults. All hardware faults must be reported through the helpdesk else there is a risk that the warranty will be invalidated or the unit further damaged.

Use of personal equipment in College (BYOD)

Advice and permission should be sought prior to using personal equipment in College. The college is not liable for any damage, or issue arising from personal equipment being used on the College network. Students are not permitted to have personal devices on the network either on the guest Wi-Fi or linked up to computers to transfer files.

Mobile Phones in School

Students are not permitted to have mobile phones in use and in view during the school day. They are allowed to keep them in their locker however whilst they are in school.

USB Memory Devices

These are permitted for use by staff, however they must have a minimum 256bit encryption on them so that confidential information cannot be accessed should the USB device be mislaid or stolen. Loss of a non-encrypted device containing confidential information will result in disciplinary action by the college.

Use of digital images

All students have permissions gathered at the start of their time at the college and these permissions must be adhered to for web and social media use and within publications in the college.

Emails, sending and using

The College email is for professional purposes only, users are only permitted to use email systems, chat rooms and other messaging methods that are approved by the school. ICT and emails for bullying or harassing others or in a way that will bring the college into disrepute will not be tolerated.

Email is a tool we need to use within our organisation and it is important that we use it correctly. Poorly worded or poorly thought out emails make us look unprofessional.

- Check your emails regularly (preferably every day), delete mails you don't need and file read emails away that you need to keep in folders
- Fill in the subject field properly, this makes it easier to find emails and search on the subject at a later date. Do not use the subject line for the whole message
- Make good use of English language and grammar; capitalise and use punctuation
- Remain professional and use appropriate language – don't use slang or TLA's (Three Letter Abbreviations) on the assumption people know what they mean – they may not
- If you are annoyed or angry, write a draft, go for a break and come back to it later- send in haste, regret at your leisure!

Good use of Calendars

- We have school calendars for resources, room bookings and minibuses – find out the names from the address book in Outlook and get used to looking at them.
- If you want to meet with someone or catch up with them – send a meeting request and their calendar will remind them.
- Use the calendars to book a room and invite people to a meeting, if things change you can send out automatic updates like time changes
- When you are away (including school holidays) - set your Out of Office Assistant if you will not be checking your emails. This helps when outside agencies or other staff members are trying to get hold of you.

e-Safety Guidance

The College has a robust set of monitoring processes within the college, however we would always recommend that if any user is in doubt, they should seek advice from the ICT helpdesk. They can advise on personal security measures, best practice and what to do if an incident occurs.

Inappropriate Use by Students or Staff

Should a staff member or a student be found to be misusing the network, then the appropriate action will be taken by the College SLT.

Secure Data Transfer in and out of the College

Any files or information of a confidential nature to be sent out on email or to another agency should always be as a minimum be zipped and password protection, the College preference is to use AnyComms via the Office Manager.

Software on all ICT Systems

The software originally installed by the school computer support staff should remain on the devices and be maintained in usable condition.

The laptops and desktops are supplied with Microsoft Windows with additional software.

Licensed software provided with all laptops and desktops includes:

- Microsoft Internet Explorer
- Microsoft Windows

- ESET Anti-Virus Software
- Microsoft Office 2013
- Policy Central

Additional Software

It is the responsibility of individual members of staff to be fully aware of additional software programs and files loaded onto their laptops and desktops. Members of staff are responsible for ensuring that only software that is licensed to their laptop or desktop is loaded onto their computers. Staff accounts will not have the relevant permissions to load software on and permission will be required from SLT to do this via the ICT helpdesk.

Upgrade versions of licensed software will be available from time to time. This will be organised by the computer support team.

School Desktops

School desktops are installed in classrooms and attached to the large display screens. These devices are fixed and should never be moved without prior agreement of the ICT support team. Any problems with or damage to the units should be reported to the ICT helpdesk.

School laptops and mobile devices

This policy applies to all laptop computers purchased by the college. A college laptop is allocated to a particular member of staff for their use as a business tool to assist in the day-to-day performance of their job.

Ellesmere College is mindful that laptop computers can be readily stolen and that the data stored on the laptop is school information, which is to be guarded against theft. Laptops are also reasonably fragile and must be treated carefully.

All laptops that are used at home, need to be covered under your personal home contents insurance or they cannot leave the site and must be stored under lock and key each evening.

College Laptops must be safeguarded:

- Against the theft of the laptop itself
- Against the theft of the information stored on the laptop (reduce the risk of the theft of information stored on the computer)
- Against any damage to the equipment (minimise the possibility of damage to the equipment)
- So that it is used to promote appropriate use

Laptops Security and Storage

The user should take appropriate security measures to protect the laptop and all its peripherals. When unattended, the laptop should be stored in a secure locked location.

Do not leave your laptops in unsupervised areas. Any laptops left in these areas are in danger of being stolen.

- Do not leave a meeting or conference room without your laptop. Take it with you
- Do not leave the laptop in your vehicle; even if the vehicle is in your driveway or garage
- Car parks are likely areas for thefts from vehicles as they provide wide choice and cover for thieves
- Never leave your laptop in plain sight

Laptop Care

A laptop is allocated to a particular member of staff for his/her use and is entrusted to their care. The member of staff should therefore take all reasonable care to secure the laptop and to guard against damage.

Carrying Laptops

- Laptops should always be within the protective bag supplied with the laptop when carried
- The carrying case can hold objects (such as folders and books), but these must be kept to a minimum to avoid placing too much pressure and weight on the laptop screen
- Laptops should be turned off properly before placing it in the carry case

Screen Care for Laptops, Desktop and Tablet Devices

The laptop screen can be damaged if subject to rough treatment. The screen is particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the laptop when it is closed
- Do not place anything in the carrying case that will press against the cover
- Do not place anything on the keyboard because forgetting objects on the keyboard and closing the lid may cause damage to the screen
- Clean the screen with a soft, dry cloth or anti-static cloth

Extreme Temperature, Magnetic Fields and X-ray

- Do be aware of the damage extreme temperature and magnetic fields can cause to computers
- Do not subject your laptop to extreme heat or cold
- Do not expose the laptop to any magnetic fields

Support

Laptops will be called in from time to time during the college year for maintenance and updates. It is expected that staff will make arrangements with the ICT helpdesk in order to do this.

Legal Property

- All laptop issued to members of staff on a short or long-term loan remains the property of Ellesmere College
- Upon termination of employment at the college, the laptop should be returned for the appropriate entry to be made in the college inventory
- Due to copyright laws, personal software should not be loaded onto the laptops

- All members of staff should comply with all trademark and copyright laws and all licence agreements

Privacy and Safety

Remember that information stored on your laptop is not guaranteed to be private or confidential.

Addendum - Guidelines surrounding ICT and Students for Staff and Parents

Inappropriate use of ICT by Students

Where a student has been using ICT (in all its forms) inappropriately, ie using foul language, sharing inappropriate content, searching for non-permitted content or wilful damage or destruction to ICT equipment then the following occurs:

- An incident is logged on the College SIMS system, Form Tutor, Head of Phase and
- Parents may be contacted
- The student's SPARC form may be updated accordingly
- Further Interventions may be applied

Security, Policy Central and Forensic Monitoring

Policy Central monitoring software is installed on all staff and student computers at the college and any concerns such as unusual web activity, gaming websites and inappropriate terminology is flagged to the college and handled as followed

- Depending on the severity of the concern the SSO (Student Support Officer) for the phase, a member of SLT (Senior Leadership Team) and or the parents may be contacted
- A SIMS incident may be logged
- Further Interventions may be applied

Mobile phones and Personal Mobile Devices

These are not permitted for use within the College, they may be brought onto site in a student's bag and left in their locker or bags for the day. Students are not permitted to make, take calls throughout the college day or take pictures or video on their phones, tablets or share content between themselves.

Internet Access Banned

In certain circumstances staff may feel that students should not access the internet within lessons and on college devices. There is a mechanism within the college to accommodate this and it can be invoked via the helpdesk.

Social Media use

Students and Parents are reminded to review security settings on social media and ensure they have the maximum privacy settings available. Students who behave inappropriately with social media may be subject to further processes with SLT and staff.

IT Curriculum – eSafety

As part of the curriculum all students will be given advice and best practice for conducting themselves online and keeping safe. If students have any concerns or worries with e-Safety, they should report them to a member of staff who will be supported by SLT and the ICT team.