Greenhills Community College

ICT Policy for Further Education Learners

GREENHILLS
COMMUNITY COLLEGE

ddletb
Bord Oideachais agus Oiliúna Dublin and Dún Laoghaire
Átha Cliath agus Dhún Laoghaire Education and Training Board

1 General

Access to Information and Communication Technology (ICT) gives learners enhanced opportunities to learn, engage, communicate and develop skills as well as enhancing their learning experience. The purpose of this policy is to provide learners of Greenhills Community College with clear guidance on the acceptable, safe and legal use of its ICT resources. This policy applies to learners using ICT resources on the College premises and remotely and is informed by DDLETB's Information & Communication Technology (ICT) Acceptable Usage Policy.

ICT resources are provided by Greenhills Community College in conjunction with DDLETB (Dublin and Dún Laoghaire Education and Training Board), SOLAS, ETBI (Education and Training Boards Ireland) and HEAnet.

ICT resources include but are not limited to:

- Desktop, laptop computers and tablets
- Audio visual equipment
- Printers and photocopiers
- Network infrastructure including cabling, WiFi access points, routers, switches and firewalls
- Digital cameras
- Equipment to support learners with additional educational needs
- Servers
- Software
- Laptop trolleys
- Online platforms, including College Website, Microsoft 365, Moodle, Adobe Creative Cloud and other online services
- Internet connection.

All computer and data resources provided by the College are the property of the College and not the personal property of individual learners.

Courses are delivered using Microsoft Windows devices. Other operating systems such as MacOS or Chrome OS are not used and will not be supported.

Learners are required to use ICT equipment and resources for **academic purposes** (learning and assessment) **only** in a safe, respectful and legally compliant manner. Learners are not permitted to use ICT equipment and resources for commercial purposes. Inappropriate use of resources exposes the College to threats including malicious attacks, compromise of systems and services and legal actions.

2 Monitoring and Data Privacy

DDLETB/Greenhills Community College reserves the right to maintain and audit activity logs and to monitor the use of its ICT resources for the following purposes:

- Maintaining the availability and performance of ICT resources
- Detecting, preventing, and investigating ICT security-related incidents
- Responding to legal or compliance requests
- Complying with legal and statutory obligations
- Investigating policy breaches

This monitoring does not constitute infringement of any individual rights to personal privacy under Data Protection and the General Data Protection Regulations. Data stored on DDLETB/Greenhills Community College's systems is the property of DDLETB/*Greenhills Community College*. Data is stored securely but in exceptional circumstances, it may be necessary for DDLETB/Greenhills Community College staff to access data.

3 Equipment Malfunction

Before using any device, a learner should check that the device is working and not defaced or damaged. If the device is malfunctioning, it should be reported immediately to the IT Co-ordinator.

Any malware, security error or warning messages or security incidents must be reported promptly by taking a screen shot of the message and emailing the IT Co-ordinator. **The original message/s should not be forwarded and the device should not be used.**

4 Student Accounts

ICT resources are provided to support teaching, learning and administrative activities. Learners are provided with accounts to permit access to ICT resources. These may include, but are not limited to:

Microsoft 365 (including Outlook email, OneDrive and Teams)
Moodle
Adobe
College server accounts
Specialist software
Printing

Learners will be issued with a Microsoft 365 account. Learners will be issued with usernames and passwords to enable access to resources.

5 Passwords and Account Security

Passwords protect the identity of each learner. Passwords must remain confidential to each learner and must not be shared with any other person. Learners must not utilise any other person's identity, attempt to exceed their assigned access rights or attempt to gain access to another user's resources or data. Learners must not attempt to bypass or probe any security mechanisms governing access to computer systems. Learners must not misrepresent themselves as other individuals, including using another user's identity.

6 Microsoft 365 Account

Learners are provided with a Microsoft 365 account. This account includes an @greenhillscollege.ie email address and access to the Microsoft Office suite of applications including Word, Excel, PowerPoint and Teams.

This email address:

- is **temporary** in nature and is provided for academic purposes for the duration of the course of study
- should be checked by learners **each College day**
- will be the **ONLY** email address used by teaching staff to communicate with learners when classes commence. Personal email addresses will not be used.

Email communication written by learners to other learners, staff, members of the College community or others must not contain remarks, content and/or images that are considered to be inappropriate, abusive, obscene, libelous, defamatory, offensive, discriminatory, harassing, pornographic, racist or threatening.

Learners must not forward emails (automatically or otherwise) to non College email systems.

Staff and student email distribution lists may only be used by teaching staff for College business.

Access to resources may be restricted based on geographic location for security reasons. Learners wishing to access their Office 365 account outside of Ireland will need to request access from the IT Co-ordinator.

7 Learners' Responsibilities

Greenhills Community College retains ownership of all accounts, data, and ICT services. Learners are responsible for all activities and information accessed using their identity.

If another user (learner or staff member) is logged onto a device, the current learner should immediately log the user out and then log in before using the device.

When finished using a device, **learners must log-out** and leave the device ready for other learners. **Failing to log out creates an unacceptable security risk.**
Learners must ensure, in so far as is practicable, that their use of these resources conforms with College policies.

Learners must not undertake or facilitate activity that could jeopardise in any way, the security (confidentiality and integrity), availability and performance of ICT resources, or compromise their utility or availability to other learners and staff etc.

Learners must not use ICT resources to: *(note: this is not an exhaustive list)*

- Steal or maliciously damage College hardware or software
- Interfere with files, system settings, network wiring, computer hardware or peripherals
- Interfere with or disable the Endpoint Protection (anti-virus and firewall) software installed on devices or knowingly introduce any virus, malware or other destructive program or device into the College network
- Access or seek to access unauthorised areas of the College's ICT resources, install unauthorised software and or connect unauthorised equipment to the College network
- Create, access, transmit, download, upload, display, print or save, any images, or material considered to be inappropriate, abusive, obscene, libelous, defamatory, offensive, discriminatory, harassing, pornographic, racist or threatening or to harass, bully, discriminate or victimise others and/or cause harm, offence, nuisance or needless anxiety to others. Particular care must be taken in relation to posts on social media platforms.
- Advocate or promote any unlawful act
- Corrupt, destroy or disrupt other learners' data or deny or disrupt services to other learners, for example, by sending unnecessary or trivial messages, chain, junk mail or unsolicited bulk or marketing email (spam)
- Plagiarise content or infringe the copyright, licence terms, trademark or proprietary rights of another person or organisation
- Deliberately misrepresent their personal views as those of the College or any other person or organisation
- Disrupt the work of other learners or teachers
- Record or photograph, without authorisation, using a personal or college device, any member of the College Community

Learners are not permitted to eat, chew gum or drink (except for bottled water) while using ICT resources.

Learners should take appropriate measures to protect their safety online including limiting the amount of personal information shared, keeping privacy settings on, creating strong passwords, taking care when downloading from the web and monitoring the amount of time spent online.

8 Software

All software provided by the College is licensed for use by current learners and may not be downloaded, stored or transferred for use by any other party. Some licences provided by the College may require learners to log in and verify their identity in order to access the software.

9 Data Retention including Saving/Backing Up Work

A learner's Microsoft 365 account includes online storage. **Learners are responsible for backing up their own data.** Learners should ensure that data stored on a local computer is either backed up automatically (synced to **OneDrive)** or backed up manually to **OneDrive** because computers and laptops may be removed from or relocated within rooms by College staff without prior notice.

Learner accounts and the data they contain are deleted at the end of each academic year. Deleted accounts include (but are not limited to) Microsoft 365, email, Moodle, Microsoft Teams, Adobe, OneDrive, SharePoint, printing and Windows accounts. Before the end of the academic year each learner should remove any data associated with their account(s). Each learner should back up the data they wish to retain to a suitable storage location separate to their College account(s).

Data on computers, laptops and tablets will be erased at the end of the academic year.

10 Equipment on Loan

It may be possible to support some learners with their studies by providing ICT equipment on loan, subject to available resources. Learners who are loaned ICT equipment are required to complete a *Device Loan Agreement (see Appendix)* and comply with the conditions of that agreement and with this policy.

Learners are responsible for the condition and security of the equipment for the duration of the loan and must report lost or stolen equipment to the IT Co-ordinator within 24 hours. Stolen equipment must be reported to An Garda Síochána and, if necessary, learners will have to ensure that relevant documentation, provided by the College, is completed. Learners must return the equipment on completion of their studies. Unreturned

equipment will be reported by the College to An Garda Síochána. Learners should be aware that Mobile Device Management software is installed on all devices for security reasons.

11 Bring Your Own Device

Learners who use their own devices in College are required to comply with this policy. These devices should be appropriately secured with Endpoint Protection (anti-virus and firewall) software. Learners must use College devices, in class, when requested to do so by teachers.

12 Reporting Requirements

Learners are required to report the following to the IT Co-ordinator:

- Equipment malfunctions
- Virus warnings, messages or security incidents
- Suspected abuse of ICT resources
- Suspected breaches of General Data Protection Regulations
- The receipt or observation of any messages, images and or content that is considered to be inappropriate, abusive, obscene, libelous, defamatory, offensive, discriminatory, harassing, pornographic, racist, or threatening.

13 Breaches of Policy

Learners should immediately report any breaches of this policy to the IT Co-ordinator.

Breaches of this policy may result in:

- The withdrawal of access to ICT resources
- Disciplinary action under the College's Code of Conduct
- Referral to An Garda Síochána or other regulatory bodies.

Glossary of Terms

Anti-virus	Software used to prevent, scan, detect and delete viruses from a computer.
Data	User data is information, material and files stored by a user.
Firewall	A network security device designed to monitor, filter, and control network traffic for protection purposes.
Hardware	Physical computer equipment (Desktops, Laptops, Printers etc).
ICT	(Information and Communication Technology) Tools and resources used to enable computing.
Malware	(Malicious Software) Software specifically designed to damage or disrupt computer systems and/or steal data.
Network	Interconnected computer hardware that can communicate with each other and share resources.
Peripheral	An accessory/component attached physically or wirelessly to computer hardware.
Router	A device that manages data traffic between devices on a network.
Server	A computer or device(s) that serve the computer network, generally storing data.
Software	Programmes installed on or used by computer equipment.
Switch	Physical or virtual devices enabling devices to communicate with each other.

Appendix

Device Loan Agreement

The ICT Policy for Learners applies to the use of devices loaned to learners. Learners should read carefully their responsibilities in relation to the use of ICT equipment under this policy.

Loan Conditions:

1. Devices (and associated peripherals, for example, a power cord) loaned to eligible learners, to facilitate engagement in their course and for the completion of coursework, remain the property of Greenhills Community College and DDLETB.

2. Devices are loaned for the duration of the academic year and must be returned to the college at the end of the academic year in May. Learners who leave their course before the end of the academic year must return the device immediately.

3. Devices must be used only by the learner and cannot be shared with or used by others.

4. Learners are responsible for the condition and security of the device in their possession and must promptly report any problems (damage, malfunction, loss, theft etc) to the IT Co-ordinator. Learners must also report stolen devices to An Garda Síochána. If necessary, learners will have to ensure that relevant documentation, provided by the College, is completed.

5. Learners are responsible for saving their data and creating their own back up before returning the device. Data on all devices will be deleted when devices are returned.

6. Learners, if deemed negligent, may be held liable for damage caused by unreasonable use, abuse, neglect, alterations, improper service, installation and improper connections with peripherals.

7. Security software is installed on laptop devices enabling them to be tracked and erased remotely.

8. Greenhills Community College will make every effort to secure the return of devices loaned to learners. In the event of non-cooperation from learners, devices will be reported as stolen to An Garda Síochána

I have read and understand these conditions and confirm my willingness to comply.