POLICY / PROCEDURE

Document Title	**ICT Acceptable Use Policy**
Version	**1.2**
Approved by	**Executive Director of Finance and Resources**
Date approved	**25 Jan 2021**
Effective date	**25 Jan 2021**
Date of next review	**26 Jan 2023**
Lead responsibility	**Technology and Innovation Manager**

1. Purpose

1.1. The purpose of this policy is to protect the organisational resources on the College Network by defining what is acceptable use of the College Network

2. Scope

2.1. This policy applies to any and all Derwentside College users of ICT equipment including employees, contractors, students, visitors and volunteers.

3. Policy / Principles

3.1. **General**

3.2. Access to all Derwentside College ICT systems and the college network is controlled by the use of College issued user IDs and passwords, all users receive a unique ID and consequently individuals are accountable for the use of their account.

3.2.1. Users will be provided with an individual account to access the network, applications and cloud environment using a unique username and password. This account will be tailored to the level of access you require and is for your use only. As such, **you must not disclose your password or security credentials to anyone**, including the IT & Innovation team. If you do so, you will be required to change your password immediately.

3.2.2. You **must not allow a student to have individual use of a staff account** under any circumstances, for any length of time, **even if supervised**.

3.2.3. When leaving a computer unattended, you **must** ensure you have either signed out of your account or locked the computer to prevent anyone using your account in your absence.

3.2.4. You will have access to personal and/or sensitive information in your role and as per the College's data protection policy, you must ensure you are following all procedures in line with the training provided and policies in place.

3.2.5. You **must not** store any College data or files on any non-college authorised system including portable storage systems (such as a USB memory stick, portable hard disk, or personal devices.) or any unauthorised third-party cloud storage (Google Drive, Dropbox or iCloud and others not approved by the College). If you need access to college data outside of the college network, please speak with the IT and Innovation team to discuss possible arrangements.

3.2.6. USB memory sticks and other portable storage devices are strictly prohibited on all College devices and systems. This is to prevent removal of College owned data, as well as to secure the network from cyber related incidents.

3.2.7. You **must not** transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the College. Please speak with the IT and Innovation team for further information.

3.2.8. When publishing or transmitting any college data, you must ensure that you are doing so in accordance with the relevant college policies on data protection and IT Security and acceptable usage.

3.2.9. If you use a personal computer or device at home for work purposes, you **must** speak with the IT and Innovation team before attempting to access College data on the device.

3.2.10. You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, mobile telephones or portable projectors) are securely stored in a locked room or cupboard when left unattended, as agreed in the device loan agreement.

3.3. Users must not:

- Allow anyone else to use their user ID to access the College Network.
- Leave their user accounts logged in at an unattended or unlocked device.
- Use someone else's user ID to access the College Network.
- Leave security credentials unprotected (e.g. writing it down).
- Perform any unauthorised changes to the College IT Systems or information. This includes changes to settings, installation or removal of software and alterations to data, hardware or connectivity.
- Attempt to access data that they are not authorised to access or use.
- Connect unauthorised devices to the College Network without prior permission from the IT and Innovation Team.

- Store any Derwentside College data on any unauthorised devices and/or equipment.
- Give or transfer any Derwentside College data or software to any person or organisation outside of Derwentside College without the appropriate authorisation.
- Create and store private data on the network.

4. Internet, Social Media and Email

4.1. Derwentside College has a duty of care to monitor and filter all web content to ensure its users are protected against unsuitable content including, but not limited to, adult material, pornography, gambling, drugs, offensive, hate, discrimination, racism, violence, terrorism, extremism and dating. Attempting to access or bypass filtering to access this content will be deemed as unacceptable use for which users will be subject to the College disciplinary procedures.

4.2. The use of the College internet and College account is intended for Derwentside College business, study and research only. All individuals are accountable for their actions on the internet and email systems.

4.3. Users must not:

- Use the internet, social media or email to access or share any material that may be considered to relate to terrorism or extremism, nor should such material be downloaded or stored on systems owned and controlled by Derwentside College.
- Use the internet, social media or email for the purposes of harassment or abuse.
- Use the internet, social media or email to engage in or support the radicalisation or potential radicalisation of any individual, whether that person(s), known or unknown are within the College or not.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images & videos) which Derwentside College considers offensive in any way. This includes, but is not limited to, sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the IT system and account in a way that could affect its reliability or effectiveness.
- Place any information on the internet that relates to Derwentside College, alter any information about it or express any opinion about the College unless they are specifically authorised to do so.
- Share any sensitive or confidential information with unauthorised parties.
- Make official commitments through the internet, social media or email on behalf of Derwentside College unless authorised to do so.
- In any way infringe any copyright, trademarks or other intellectual property including downloading or accessing copyrighted material such as music and video files, books and publications (not an exhaustive list) without appropriate approval.
- Download, run or install any unauthorised code, scripts or executables or software.

5. Monitoring and Filtering

5.1. All device and account usage including Internet access is monitored, filtered and logged. An investigation will be triggered where reasonable suspicion exists of a breach of this or any other policy or appropriate law. Derwentside College has the right to monitor activity on its systems, including internet and email, in order to ensure network security is maintained and effective operation and to protect against misuse.

5.2. Repeated attempts to gain access to restricted content will be reported to the relevant parties.

5.3. On occasion a user (over the age of 18) may need access to materials that would otherwise be deemed as unsuitable for the purposes of study and research. A request stating the reason and the type of content required must be forwarded to the IT and Innovation Team who will review the requests and where necessary, seek SMT authorisation to allow access and the period of time access will be permitted.

5.4. All personal (Bring Your Own Device – BYOD) devices that are connected to the College Wi-Fi network are subject to the same monitoring, filtering and logging as college owned devices.

6. Privacy

6.1. Use of the College IT Network, including your email account and storage areas provided for your use, may be subject to monitoring by the College to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the college network and Azure platform does capture historical and current web browsing history, cookies, usernames and passwords and any active logon sessions.

6.2. Use of a personal device with a college issued account, will be scanned for security compliance, which includes retrieving a list of installed applications and programs, current operating system versions and capturing security information such as boot operations and the use of a secure complex password.

6.3. Storage of sensitive personal information on the College network and account that is unrelated to college activities (including personal files, personal passwords, photographs, or financial information) is strictly forbidden. Storage of such files on the College network and/or account will be captured by the relevant security systems in place.

6.4. The College may also use measures to audit the use of College IT Network and devices for performance and diagnostic purposes.

6.5. **Use of the College IT system and College issued account indicates your acceptance of the above monitoring taking place.**

7. Remote access

7.1. Remote access to some College systems, services and resources is possible from authorised devices only where this has been granted by the IT and Innovation team. Remote connections are considered direct connections to the network. As such, you are subject to the same conditions, requirements, and responsibilities of this policy. All connections are logged for security monitoring.

8. Use of your own equipment

8.1. Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) and must not be used until approved. This test must be performed at regular intervals as required by the College policy on electrical safety testing.

8.2. You **must not** connect personal equipment to College IT equipment without prior approval from the IT and Innovation team, including mobile phones or portable storage devices such as USB memory sticks.

9. Conduct

9.1. You **must** at all times conduct your IT usage professionally, which includes being polite and using the system in a safe, legal, and business appropriate manner. Usage is in accordance with the college values and any applicable policies. Among uses that are considered unacceptable are the following:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You **must** respect, and not attempt to bypass security or access restrictions in place on the IT Network

9.2. You must not intentionally damage, disable, or otherwise harm the operation of the IT Network and devices.

9.3. You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:

- Excessive downloading of material from the Internet;
- Excessive storage of unnecessary files on the network storage areas;
- Use of printers to produce class sets of materials, instead of using photocopiers.

9.4. You should avoid eating or drinking around IT equipment and when using or transporting portable devices such as laptops and iPads. Food and drink is strictly prohibited for both staff and students in all IT Classrooms and the LRC.

10. Reporting problems with the IT network, systems, services and devices

10.1. It is the job of the IT and Innovation team to ensure that the College IT Network and devices are working optimally at all times and that any faults are rectified as soon as possible. To this end:

- You should report any problems that need attention to a member of the IT and Innovation Team as soon as is feasible. Problems that seriously hinder your role or teaching and require immediate attention should be reported by telephone or email; any other problem **must** be reported via the online helpdesk system.
- If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of the IT and Innovation team **immediately**.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable.

11. Definitions

11.1. Device is defined as, but not limited to, the whole workstation and any mobile device e.g. laptop, printer, notebook, tablet, smartphone, smart watch and includes any virtual computers and network attached storage.

11.2. The College Network is defined as the internal LAN network on College premises and all college owned devices. Including but not limited to:

11.3. The VoIP Telephony system, mobile phones, Servers, desktop PC's, laptops tablets, printers, photocopiers, network switches, cabling, Desktop PCs, Monitors, peripherals, Azure-joined devices and the College Cloud environment.

11.4. Peripherals are defined as but not limited to; Monitor, keyboard, mouse, speakers, headphones, disk drives, optical drives, webcams and any associated cables or leads.

11.5. College User ID is defined as the college issued log on ID, Microsoft 365 email and Azure Active Directory account.

12. Accountability

12.1. The Technology and Innovation Manager is responsible for the drafting and implementation of this policy.

12.2. He or she is also responsible for ensuring that this document is regularly reviewed and updated – and is the first contact point for managers seeking advice and guidance about the ICT – Acceptable Use Policy or making enquiries about its interpretation.

12.3. All managers are responsible for ensuring that they and their team members follow the requirements set out in this document.

12.4. All employees and learners are responsible for adhering to the requirements set out in this document.

13. Equality & Diversity

13.1. The College has paid due regard to equality considerations during the preparation and implementation of this Policy and Procedure.

13.2. These considerations included the potential for any differential negative effect on the grounds of age, disability, gender reassignment, pregnancy and maternity, race (including ethnic or national origins, colour or nationality), religion or belief (including lack of belief), sex, sexual orientation, marriage or civil partnership.

13.3. The College's judgement is that there is no such negative effect on those grounds and, consequently, no potential breach of the Equality Act 2010.

13.4. The operation of this Policy and Procedure will be monitored by the Personnel Manager in order to establish that no unlawful discrimination is taking place and to identify opportunities for the College to enhance equality of opportunity and fair treatment.

14. Review

14.1. This document will be reviewed by February 2023.

14.2. The Technology and Innovation Manager will undertake this review, taking into account the outcomes of the monitoring process, legislative changes and developments in good practice.

14.3. As part of the review, the Technology and Innovation Manager will seek and consider the views of the College's employees and of the recognised trade unions.

14.4. The outcome of the review will be reported to the Senior Management Team.

15. Document Identification

Category [select ONE only]	☐Programmes/courses ☐Partnerships ☐Finance ☐Quality ☐Governance ☐Health and safety ☐Facilities ☒IT and Innovation ☐MIS ☐Admissions ☐Teaching and learning ☐Personnel
Audience [select ALL that apply]	☒Employees ☒Learners ☐Partners ☐Suppliers