



POLICY / PROCEDURE

Document Title	ICT Acceptable Use Policy
Version	1.1
Approved by	Executive Director of Finance and Resources
Date approved	06 Feb 2019
Effective date	06 Feb 2019
Date of next review	06 Feb 2021
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

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

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 computer.
- Use someone else's user ID to access the College Network.
- Leave their password unprotected (e.g. writing it down).
- Perform any unauthorised changes to the IT systems or information. This includes changes to settings, installation or removal of software and alterations to 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 IT and Innovation
- Store any Derwentside College data on any unauthorised equipment.
- Give or transfer any Derwentside College data or software to any person or organisation outside of Derwentside College without the appropriate authorisation from a line manager.
- Create and store private data on the network.

3.2. Internet, Social Media and Email

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.

The use of the College internet and email is intended for Derwentside College business, study and research. Occasional moderate personal use is permitted where such use does not affect the individual's business / learning performance, is not detrimental to Derwentside College in any way, does not breach any term and condition of employment or learner agreement and does not place the individual or Derwentside College in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

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 mail system in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- 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.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet, social media or email on behalf of Derwentside College unless authorised to do so.
- Download copyrighted material such as music media (mp3 and other) files, film and video files, book and publications (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any malicious code, scripts or executables.

4. Monitoring and Filtering

- 4.1. All 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. Derwentside College has the right to monitor activity on its systems, including internet and email in order to ensure network security and effective operation and to protect against misuse.
- 4.2. Repeated attempts to gain access to restricted content will be reported to the relevant department or head of faculty.
- 4.3. 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 Technology and Innovation Manager who will seek SMT authorisation to allow access and the period of time access will be permitted.
- 4.4. All personal (Bring Your Own Device – BYOD) computers that are connected to the College Wi-Fi network are subject to the same monitoring, filtering and logging as College owned computers

5. Definitions

- 5.1. Computer is defined as the whole workstation, (Base unit, keyboard, mouse, speakers, headphones, disk drives, optical drives, etc.) or any mobile device (laptop, notebook, tablet, smartphone, etc.) and includes any virtual computers and network attached storage.

6. Accountability

- 6.1. The Technology and Innovation Manager is responsible for the drafting and implementation of this policy.
- 6.2. 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.
- 6.3. All managers are responsible for ensuring that they and their team members follow the requirements set out in this document.
- 6.4. All employees are responsible for adhering to the requirements set out in this document.

7. Equality & Diversity

- 7.1. The College has paid due regard to equality considerations during the preparation and implementation of this Policy and Procedure.
- 7.2. 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.
- 7.3. 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.
- 7.4. 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.

8. Review

- 8.1. This document will be reviewed by February 2021.
- 8.2. 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.
- 8.3. 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.
- 8.4. The outcome of the review will be reported to the Senior Management Team.

9. Document Identification

Category [select ONE only]	<input type="checkbox"/> Programmes/courses <input type="checkbox"/> Partnerships <input type="checkbox"/> Finance <input type="checkbox"/> Quality <input type="checkbox"/> Governance <input type="checkbox"/> Health and safety <input type="checkbox"/> Facilities <input checked="" type="checkbox"/> IT and Innovation <input type="checkbox"/> MIS <input type="checkbox"/> Admissions <input type="checkbox"/> Teaching and learning <input type="checkbox"/> Personnel
Audience [select ALL that apply]	<input checked="" type="checkbox"/> Employees <input checked="" type="checkbox"/> Learners <input type="checkbox"/> Partners <input type="checkbox"/> Suppliers