Derwentside College

Acceptable Usage

Effective from: 26/01/2025

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

Users must:

- Use IT resources for educational, research and administrative purposes only.
- Protect login credentials and ensure their confidentiality.
- Adhere to intellectual property laws and licensing agreements.
- Adhere to data protection and privacy regulations, such as GDPR.
- Use College IT resources in a manner that does not compromise the rights of others or disrupt the educational environment.
- Report any IT security breaches or suspicious activities promptly.

Users must not:

- Access, create, or distribute offensive, obscene, or discriminatory content.
- Use IT resources for personal financial gain or unauthorised commercial activities.
- Attempt to bypass or disrupt security protocols, including hacking or introducing malware.
- Share login credentials or access unauthorised systems or data.
- Use IT resources to harass, bully, or impersonate others.
- 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 the College.
- 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.
- Access, download, send or receive any data (including images & videos) which the College considers offensive in any way. This includes, but is not limited to, sexually explicit, discriminatory, defamatory or libelous material.
- Use profanity, obscenities, or derogatory remarks in communications.
- Use the email 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 the College, alter any information about it or express any opinion about the College unless they are specifically authorised to do so.
- Make official commitments through the internet, social media or email on behalf of the 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.
- Leave their password unprotected (e.g. writing it down).
- Connect unauthorised devices to the College Network without prior permission from the IT and Innovation Team.
- Store any College data on any unauthorised equipment.
- Give or transfer College data or software to any person or organisation outside of the College without the appropriate authorisation from a line manager.
- Create and store private data on the network.