DCG

DERBY COLLEGE GROUP
POLICY

Information Technology Student Acceptable Use Policy

Policy Number:	ITS-004
Executive Owner:	Deputy CEO
Owning Strategy / Department:	IT Services
Approval Board / Committee / Group:	Corporate & Student Support Services Leadership
User Group:	DCG Employees
Relevant To:	All College Students and other users of the IT facilities
Implementation Date:	August 2011
Approval Date:	June 2020
Next review Date:	October 2026

Date:	October 2023
Ref:	IMC
Originator:	Director of IT Services
Area:	IT Services

Once printed, this is an uncontrolled document. Refer to Policy Portal for latest version.

POLICY - PROCEDURES - GUIDELINES - RELATED DOCUMENTS

Policy Accountability and Implementation

Policy Title:	Information Technology Student Acceptable Use Policy
Policy Author / Reviewers:	Director of IT Services
Policy Implementation:	Director of IT Services
Policy Monitoring and Compliance:	Director of IT Services
Policy Review Timeline:	This policy will be reviewed every three years or sooner subject to any legislative / contractual or College re-organisation.

Synopsis:
This policy provides a framework for students to govern the responsible use of the IT services.

Policy Classification and Publication

Classification

- Strongly Recommended (SR)

Publication

- Intranet – Policy portal
- Student VLE (Moodle)

Empowering/related legislative and/or authoritative references:

Data Protection Act 2018, Copyright, Designs and Patents Act 1988, Protection from Harassment Act 1997, Communications Act 2003, Malicious Communications Act 1988, Public Order Act 1986, Obscene Publications Act 1959 and 1964, Protection of Children Act 1978, Sexual Offences Act 2003, Sexual Offences Act 2003 Memorandum of Understanding and the Computer Misuse Act 1990, Terrorism Act 2006, Prevent Strategy 2011.

Impact Assessment reference: IA28 2011

Periodic Policy Review / Change History

Note: Please make it clear if change/review relates to procedures, guidelines and associated documents only or it is a rational for a new or substantive policy review

Version	Reviewed / Modified by:	Change History	Advisory committee / groups or specialists	Review / Meeting Date/s
1.1	Director of IT Services	Minor alteration following legislative change	Deputy CEO	June 2020
1.2	Director of IT Services	No changes	N/A	Oct 2023

1. Policy Statement

Derby College actively encourages the use of Information Technology by students as a valuable tool to enhance and support their learning.

This policy provides a framework for students to govern the responsible use of the IT services to ensure they are used:

- Appropriately
- Effectively
- Legally
- Securely
- Without undermining the College
- In a spirit of cooperation, trust and consideration for others

2. Definitions

The use of College provided network systems and services, including but not limited to, Internet, intranet, email and SMS services.

3. Principles

General Principles

- College provided Internet/intranet and email privileges are considered College resources and are intended to be used for educational purposes only. Usage will be monitored for unusual activity.
- Correspondence via email cannot be guaranteed to be private and the College will add disclaimers to all outgoing email.
- Use of Internet/intranet and email will be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources. Internet usage will be proactively monitored to detect any material promoting terrorism or radicalisation as covered by the Terrorism Act 2006 and the Prevent Strategy 2011.
- The distribution of any information through the Internet, computer based services, email and messaging systems is subject to scrutiny. The College reserves the right to determine the suitability of this information.
- The College will monitor internet usage to encrypted or secure websites. In line with industry standards and best practise the College will intercept, decrypt and interrogate web traffic to identify categories and content for monitoring purposes. The only exceptions to this are where the traffic is categorised as banking or healthcare. In such instances no content will be tracked as it may expose personal or sensitive information.

Conditions of Use

These guidelines apply to all computers, mobile devices, software and data within the college; or belonging to the college but located elsewhere. It includes the use of Student Portal/Moodle. It covers remote access from outside of the college, regardless of which device is used to make the connection e.g. personal computer at home, mobile phone.

These resources are provided on the understanding that they are not misused in a way that will interfere with, disrupt or prevent anyone from legitimately using college resources.

You may use your personal laptop or other mobile device to connect to the college wireless network but you must ensure that the appropriate anti-virus / anti-malware protection is installed.

Use of the IT facilities is subject to the provisions of the Data Protection Act 2018, Copyright, Designs and Patents Act 1988, Protection from Harassment Act 1997, Communications Act 2003, Malicious Communications Act 1988, Public Order Act 1986, Obscene Publications Act 1959 and 1964, Protection of Children Act 1978, Sexual Offences Act 2003, Sexual Offences Act 2003 Memorandum of Understanding and the Computer Misuse Act 1990, Terrorism Act 2006, Prevent Strategy 2011.

Users shall not:

- Visit Internet sites that contain obscene, hateful or other objectionable materials as defined in the Internet Site Criteria document; send or receive material that is obscene or defamatory or which is intended to annoy, harass or intimidate.
- Use the Internet or email for any illegal purpose.
- Represent opinions as those of the College.
- Make or post indecent remarks, proposals or materials.
- Install any software onto College equipment.
- Any material promoting terrorism or radicalisation as covered by the Terrorism Act 2006 and the Prevent Strategy 2011.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging either to parties outside of the College or to the College itself.
- Download any software or electronic files without implementing virus protection measures that have been approved by the College.
- Intentionally interfere with the normal operation of the network, including, but not limited to, propagation of computer viruses and sustained high volume network traffic which substantially hinders other users in their use of the network.
- Examine, change or use another users files, output or user name for which they do not have explicit authorisation.
- Perform any other inappropriate uses identified by the College.

Users who violate any of the guidelines set in this policy may be subject to disciplinary action. The College also retains the right to report any illegal violations to the appropriate authorities.

4. Scope and Limitations

This policy applies to all Derby College students and governs their use of any College devices capable of accessing electronic systems, including but not limited to; desktop and laptop computers and tablet devices.

For the equivalent policy applicable to staff, please refer to the Information Technology Staff Acceptable Use Policy.

5. Responsibilities

Responsibility for the creation and implementation of this policy lies with the Director of IT.

6. Implementation Arrangements

Students are made aware of this policy during their induction and a copy is available on Moodle. Students are also subject to e-safety training in line with the college e-safety policy.

7. Monitoring and Review

This policy will be reviewed on a three yearly basis and updated as necessary to reflect any technological, legal or other relevant developments.

8. Guidelines

There are no separate guidelines in relation to this policy.

9. Procedures

There are no separate procedures in relation to this policy.

10. Templates / Forms

There are no separate templates or forms in relation to this policy.

11. Related Documents

- E-safety policy
- Copyright policy