POL-001 - ACCEPTABLE USE OF IT – STUDENTS POLICY

Document reference	2515
Version number	012
Owner	Louise Jones
Department/Area	IT Services
Date of review	10.04.24
Date of approval	24.04.24
Approved by	SLG
Next review date	23.04.26
Date of EIA if appropriate	03.04.24
Status (delete as appropriate)	Internal/Public

Scope

This policy lays out the responsibilities associated with student access to Dudley College IT Hardware, software, Network, Internet Connections, Systems and Equipment. This policy importantly links to other policies and procedures to ensure a full understanding of responsibility is understood by users.

Introduction

By logging on and using any of the college computer equipment or systems you are agreeing to this policy.

If you are unsure about anything in this policy, please speak to your course tutor or contact the Duty Manager, who may then need to discuss this with the college IT department.

In accordance with Safeguarding and Counter Terrorism legislation all student computer activity is tracked and monitored. Use of Office 365 (including Teams) on your personal device is also within scope. The college has a legal and moral responsibility investigate suspicious activity and share the information with the relevant authorities. Students should also be aware that there could be difficulty in differentiating online research for genuine curriculum reasons.

1. JANET Internet Connection

All access to the Internet from the college is supplied by JANET (Joint Academic Network). As such, all users in the college must adhere to their Acceptable Use Policy, which can be viewed at:

https://community.jisc.ac.uk/library/acceptable-use-policy

The terms of this policy are in addition to and take precedence over this college policy.

2. Access to IT

Every student is issued with a login for the college network once their enrolment has been fully completed. Multi-Factor Authentication (MFA) is mandatory for all IT accounts. MFA is in place to safeguard you and the college against external cybersecurity threats. You will need a secondary device to authenticate your access to systems when not in college.

This can be an authenticator app on your smartphone, email to a personal account, text message or telephone call. If you don’t have access to any of these, please speak to your tutor about logging a request with the IT Helpdesk for a special MFA token. You will not be prompted for MFA whilst using a college computer. MFA is required if you bring your own device to college and connect to the EDUROAM network.

A college IT account includes access to the college's Microsoft 365 tenant including:

a. Microsoft Office Online
b. Microsoft OneDrive
c. Microsoft Teams

You will receive 5TB of cloud storage on your college OneDrive to store your work. Please ensure you keep back-ups of any important data or files in a separate location. Your college IT account is also enabled for Single-Sign-On & Same-Sign-On with some college systems including:

d. Office 365
e. MyDudleyCollege
f. ProPortal

It is your responsibility to keep these login details safe and not to access systems with any login details other than your own.

The basic security rules are:

- Do not give your login details for the network or any college system to anyone else.
- Do not attempt to log into the network or any college system with any login ID other than your own.

3. Acceptable Use of IT

The college systems offer a wide range of learning and communication tools, and you are encouraged to make full use of these. However, this usage must not damage college equipment or systems, cause offence or harm to others or infringe any laws.

- Do not send any communication or view sites which could be considered offensive, obscene, libelous, sexist or that incite racial hatred. Even if you forward on a message written by someone else you will be open to disciplinary action.
- Do not download or install any software onto college computers without the permission of your tutor and only in direct relation to your studies. This includes games software.
- Do not use college equipment to copy copyright-protected material or engage in any illegal activity.
- Do not attempt to access, edit, move or delete system files/programs or adjust the settings on college computers or systems.
- Do not attempt to penetrate the security of any college systems.
- Do not knowingly connect any device to college equipment which has a virus or other malicious software installed or send such files via electronic communication.
- Always use college equipment with care to avoid any unnecessary damage.
- Your access to the Internet is filtered to stop access to sites which are inappropriate to college studies. Do not attempt to bypass this system. If you feel you need access to a site that is being blocked, please speak to your course tutor.
- Always be respectful to staff and students on Microsoft Teams and other online

learning platforms. Any misuse or misbehaviour on Microsoft Teams is logged and alerts the Safeguarding Team.

- Do not attempt to access information on radicalisation and any other terrorist activities unless it is a genuine part of your curriculum and you have been requested to do so by your tutor.

4. Staying Safe Online

Every student has a right to feel safe when they are online, and it is your responsibility to behave responsibly and ensure you are doing all you can to avoid being a victim of cybercrime.

- Do not use any electronic system (college owned or otherwise) to bully, harass or intimidate others.
- Do not use any electronic system (college owned or otherwise) to promote intolerance or recruit others to violent or extreme ways.
- When using public social networking tools, even those built into college systems such as Microsoft 365, do not share your personal information.
- If you are a victim of any inappropriate behaviour or witness it happening to others, you must inform your course tutor.

5. Personal Drives and External Access

Certain areas of the college allow you to connect to the internet using your own portable devices via Wi-Fi. In addition, several college systems can be accessed from anywhere with an Internet connection (not just inside college).

- When using the college Wi-Fi connection, you are subject to the same conditions laid out in this policy, even when using your own device.
- If you are using any college system, even when not in college, you are still subject to the same conditions laid out in this policy. For example, a student sending an offensive message to another student in their own time on their own PC but through a college system such as Teams would still be subject to disciplinary procedures.
- Logging into Microsoft 365 through a VPN (Virtual Private Network) or other anonymiser software will result in your account being blocked.

6. Borrowing College IT Equipment

- Some learners may be eligible for a college device through government or college led schemes.
- Students may need to confirm their eligibility with the Learner Finance team.
- A record of the device loan will be kept by the college. You will receive communication when the device needs to be returned to college.
- Unless explicitly stated any loaned devices are treated the same as college computers.
- You are responsible for ensuring the physical welfare of the device. If any evidence of deliberate physical damage is found, you will be subject to disciplinary procedures.

7. Monitoring

In accordance with the **Prevent Duty** and **Keeping Children Safe in Education** the use of IT systems is proactively monitored to keep everyone in the college safe, including visited websites, images viewed, keystrokes, Microsoft Teams activity and computers accessed. Alerts for critical and high-risk events are immediately emailed to the Safeguarding team.

Using college owned IT equipment to research terrorism and counter terrorism as part of your course might be flagged for review by the Safeguarding team. You may need to provide a justification as to why such resources are being accessed and their relevance to your studies.

If we have evidence of any learner conducting an attack against the college network, you will be subject to disciplinary measures outlined below. This list is not exhaustive, but learners should take note that the college takes cybersecurity incidents very seriously.

Severity 1	**Immediate & Permanent Exclusion.**
Protocol Attacks / Denial of Service Attack	Targeting college systems, servers, or networks and flooding them with traffic to exhaust their resources and bandwidth.
Packet Sniffing i.e. Wireshark	Gathering, collecting, and logging some or all packets that pass through a computer network.
Crypto jacking	Using malicious code to mine crypto currencies.
Ransomware Injection	Encrypting college data in exchange for payment or favour.
Use of known "Bad USB"	Using a re-programmed USB device to discreetly run malicious commands or programs on college computers.
Use of Advanced Persistent Threat	Setting up unauthorised long term remote access on a college computer.
Use of Etherkillers on IT equipment.	Plugging in an etherkiller cable into college equipment to inflict serious physical damage.
Use of Kali Linux or similar tools on the college network	Using hacking and penetration testing tools against all parts of the college network.
Zero Day Exploits	Targeting a college system or server with a known and unpatched vulnerability.
Use of "Wi Fi Pineapple" / "WiFi Coconut"	Conducting penetration tests on the college's Wi-Fi Infrastructure.
SQL Injection Attack	Using SQL to attack a database-driven website through injection of malicious code.
Spoofing	Impersonating someone or something to access sensitive information and carry out malicious activities.
Connecting personal device to college network via ethernet cable to maliciously harm college network	Attempting to connect your device to the college network and attempting to carry out an attack against the college network.

Severity 2	Stage 3 Disciplinary
Malware Attack – Attempting to inject malware onto college computers using software development tools or a premade package disguised as legitimate software.	Including Worms, Viruses, Trojan Horses, Emotet, Botnets, Fileless Malware, Spyware, Rootkits, Bots to maliciously damage college computer systems.
Anti-Virus Tampering	Deactivating or circumventing anti-virus controls on college systems.
Privilege Escalation	Gaining unauthorised higher-level access on a college computer or system.
Downloading Copyrighted Content	Downloading copyrighted music, movies, video games or TV shows without permission is illegal. It's also against the law when you share these files with someone else, even if you aren't aware that you are even sharing illegal content.
Angler Phishing Attack	Using social media platforms to gets victims to unknowingly give away sensitive information.
Whale Phishing Attack	Targeting high profile individuals such as CEO's or celebrities using sophisticated social engineering techniques to get sensitive information.
Spear Phishing Attack	Targeting specific individuals within a company to get sensitive information.
Brute Force Attack	Trying all possible password combinations to gain unauthorised access to college systems or sensitive data.
Cross Site Scripting Attacks	Injecting malicious code into a legitimate web page or web application.
Backdoor Exploitation	Using malicious code to sidestep normal authentication procedures.
AI powered Attacks	Using artificial intelligence to carry out an attack on college systems.
Dictionary Attack	Attempting to guess passwords into college systems by trying many common words and their variations.
Identity Based Attack	Credential Stuffing / Golden Ticket Attack & Kerboroasting are all prohibited on the college network.

Severity 3	Stage 2 Disciplinary
Shoulder Surfing	Spying on unsuspecting victims to collect data such as passwords, pins and other login information.
DNS Poisoning	Manipulating DNS records to redirect towards a malicious website.
Hosts File Manipulation	Editing the hosts file for malicious activity such as redirecting web addresses to fraudulent sites or blocking access or anti-virus update servers.
Social Engineering	A manipulation technique that exploits human error to gain access to sensitive information or systems.
Attempting to / Successfully connecting personal a device to the college network via ethernet	Personal devices must not be connected to the college network via ethernet.

The following Associated Documents can be requested.

POL-002 - Staff IT policy
POL-016 - Safeguarding
POL-019 - Social Media
POL-028 - Data Protection
Conduct - Student procedure
Blended Learning procedure
Safeguarding - Children & Adults procedure
Prevent Radicalisation Extremism Strategy procedure

Policy Review

This policy will be reviewed every two years.