# IT Acceptable Use Policy (Staff, Governors & Visitors)

# IT Acceptable Use Policy
# (Staff, Governors & Visitors)

## Document Change Control:

| Author | Version | Date Issued | Change |
|---|---|---|---|
| Director of IT | 0.1 | 30/08/2019 | Initial Draft |
| Director of IT | 0.2 | 02/09/2019 | Addition of section 10, 11, 12 |
| Director of IT | 0.3 | 09/10/2019 | SMT Approval given |
| Director of IT | 1.0 | 15/09/2019 | Document published |
| Director of IT | 2.0 | 01/03/2021 | Remote Working Additions |

# Contents

## 1. Introduction

1.1 The aim of this policy is to ensure that the college's IT facilities are used safely, lawfully and fairly by all its stakeholders within the college. The college seeks to promote the proper use of IT to facilitate effective learning and teaching as well as to ensure the effective use of IT in its business function.

1.2 This policy is not exhaustive and in some circumstances there will not be specific guidelines to follow. In these instances best judgement should be used in line with industry standards or seeking advice from the college IT Services.

1.3 By accessing or using the IT facilities at the college you agree to be bound by this policy and all related security policies.

1.4 Any breach of this policy will be reviewed and may be deemed as gross misconduct and will be dealt with under the staff disciplinary policy.

1.5 In addition to this policy all users must also comply with the JANET Acceptable Use Policy, available at https://community.ja.net/library/acceptable-use-policy.

## 2. Scope

2.1 This policy applies to the use of all IT facilities by staff, governors and visitors of the college (visitors may not receive the same levels of access but are still bound by the policy). All users affected by this policy must comply and failure to do so may lead to disciplinary action.

## 3. Definitions

| Term | Definition |
|---|---|
| **Staff** | Any person that is instructed to work for or on behalf of the college be it paid or voluntary |
| **IT Facilities** | Hardware, software, data, network access, telephony, services provided by licensed third parties, online cloud services or using college IT credentials**;** whether they are provided**,** or arranged**,** by IT services**,** by individuals**,** or by other professional services |
| **Software** | This defines any software across the college including operating systems, applications, databases and platforms. |
| **SSID** | Server Set Identifier – When you search on your mobile device, they are the different Wi-Fi connections available. |
| **VPN** | Virtual Private Network – These are applications that can be purchased and used to secure internet traffic on public Wi-Fi |
| **Password Manager** | This is an application that you can secure your passwords in. It uses on secure password or biometric ID so you only need to remember that password to gain access to all your other saved passwords. |
| **SCCM** | This is a program used by the IT Services to deploy software and update to all computers. |

| | |
|---|---|
| **Visitor** | Any person who interacts with the college IT equipment with permission from the college. |

## 4. General Use

4.1 You must not connect any personally owned device to any part of the internal network that has not be provided specifically for that purpose. It is allowed to connect personally owned devices to the college Wi-Fi network on certain SSID's provide by the college. This does not apply to remote access or internet enabled services.
4.2 You must not attempt to circumvent, evade or defeat any security and audit controls in any way.
4.3 You must not deliberately introduce any software into the college designed to cause harm or bypass the college IT infrastructure security or data.
4.4 You must report any suspicion, caution or incident of a virus, phishing attempt, persistent spam or hacking attempt to the IT Support service as a matter of urgency.
4.5 You must not leave your computer or device unattended without locking or logging off.
4.6 You must not install any software or hardware to any device owned by the college. Only software made available to you through the SCCM software catalogue has been approved by IT Services can be installed by the user.
4.7 You must not use the IT facilities for playing games, or any non-business activity that may cause strain on the device or network e.g. bitcoin mining.
4.8 All users have the responsibility to report any damage or suspicious behaviour to the college IT facilities. All issues should be reported to the college IT service desk.
4.9 Learners should never be left unattended in a PC classroom. If any damage occurs as a result of learners being left unattended, the curriculum department concerned are liable to provide the costs for replacing damaged IT equipment.
4.10 The college reserves the right to withdraw or block any IT facility to any individual or group without notice due to misuse, security precautions or breach of policy.

## 5. User Identification

5.1 All users will be given a unique user account for individual use. This account will be used at the college for use of identification and access to different areas of the IT network.
5.2 Users are responsible for their own network account and any activity associated on that account. You must not use anyone else's account, nor must you allow anyone else to use your account.
5.3 You must not share your account details with anyone else. Anyone asking for your account details are to be considered fraudulent. IT Services will never ask for your password.
5.4 If you believe your account to be compromised, you must change your password straight away. It is recommended that you change your password annually.
5.5 Password security requirements define that you must have a strong password (recommended 14 or more characters long; must contain three of the following character definitions: uppercase, lowercase, number and symbol; must not contain a

significant portion of your username and may not be one of the last 4 passwords you have used).

5.6 You must not use the password you have for you college account for any other purpose be it personal or business use.

5.7 All common or easily guessed passwords are not to be used. Common passwords are passwords that have any relation to the user e.g., pets name etc or easily guessed passwords such as 'Businessname1'.

5.8 It is recommended that you use a passphrase which could be three random words mixed with symbols and numbers to makes it easier to remember. As an example, taking the words Football, School and Sandwich to create FooTball$chool!SandWich%

5.9 You must not write down or store your password in plain text (unencrypted). If you are struggling to remember passwords, then you should look at using a password manager.

## 6. Email, Electronic Communication & Storage

6.1 All electronic communication will be conducted in a way that is professional and appropriate for its intended recipient. Employees should ensure that the content of the communication reflect the college's Value, Ethics and Code of Conduct.

6.2 All external college communication should include either the senders name or a means for the recipient to get in contact with the college.

6.3 Users must not use their college electronic contact details for signing up to anything that does not relate to college business.

6.4 It is the responsibility of the sender to make sure that the correct level security is applied to content leaving the college. Email is not a secure medium and if confidential data is being sent then extra encryption may need to be used.

6.5 Users must be aware that although electronic communication is useful it does come with its risks of mistaken use. Users must ensure that they are sending messages to their intended recipients.

6.6 It is the responsibility of user to make sure that their electronic communication platforms are correctly managed. This includes using 'out of office' messages when not available, maintaining a tidy mailbox and deleting messages that are no longer relevant.

6.7 The creation of material that is discriminative, offensive, indecent, threatening, abusive, and obscene, violates the privacy of others or brings the college into disrepute on any grounds is strictly prohibited.

6.8 It is the responsibility of the user to keep their digital work areas tidy and with data that is still current and relevant. Data retention policies apply and if you delete files, after a certain period you may not be able to get them back. Each user has the use of a 2GB home drive and a 1TB OneDrive storage that they must individually maintain. This amount of allowed storage means there is no need for external storage devices to be used.

6.9 College telephone handsets and lines are provided for business use. Personal telephone calls must be kept to a minimum and, preferably, only made during designated break periods. It is recognised, however, that staff members will need to make emergency calls occasionally. All international calls can only be made after gaining authorisation from the immediate line manager beforehand. The college recognises, however, that some staff members make international calls for college business.

## 7. Monitoring & Privacy

7.1 The college undertakes some routine monitoring of activity on the ICT facilities to ensure that they operate correctly and to protect against the risk of harm from viruses, malicious attack and other known threats. This does not normally involve the monitoring of individual communications or the disclosure of the contents of any user files.

7.2 The college reserves the right to monitor your use of the IT facilities including communications sent and received, internet services accessed, files uploaded/downloaded or stored:

7.2.1 to protect the IT Facilities against viruses, hackers and other malicious attack;

7.2.2 to assist in the investigation of breaches of this and other relevant college policies;

7.2.3 to prevent or detect crime or other unauthorised use of the IT Facilities;

7.2.4 when legally required to do so, for example as part of a police investigation or by order of a court of law;

7.2.5 where such monitoring is necessary, to pursue the college's other pressing academic and business interests, for example by reviewing the emails of employees on long-term sick leave or to disclose documents under the Freedom of Information Act 2000/GDPR.

7.3 Monitoring or access to an individual's email account, content, service or data supplied by the college shall only be carried out if authorised by the Director of IT and the Director of HR for members of staff, visitors and third parties. Reasons for this may include business continuity, staff absence or alleged malpractice. Once approved, the access will be given to the line manager or other senior management team members.

7.4 Any information collected during the course of the monitoring will be held securely. You will be given the opportunity to see and explain any data collected, as part of any disciplinary or grievance procedures that may result.

## 8. Legal Requirements

8.1 You must not use the IT facilities in any way that could expose you or the college to any criminal or civil liability.

8.2 You must only use the IT facilities in accordance with the following legal procedures and policies.

8.2.1 Computer Misuse Act 1990

8.2.2 Data Protection Act 2018

8.2.3 Communications Act 2003

8.2.4 General Data Protection Regulations

8.3 You must not use the IT facilities to access store or distribute material that is offensive, indecent or pornographic. Due to the nature of the college and it being in the education setting there may be exceptional circumstances where material that falls under the above heading may be needed for teaching purposes. If this is the case then access to this material must not conflict with point 8.1.

8.4 In compliance with Counter-Terrorism and Security Act 2015 and the Prevent regulations, users must not create, transmit, receive view or store material with the intent to radicalise themselves or others. If any content that may fall under this

heading is needed in any teaching material then written authorisation must be given by the DSL and the Director of IT.

8.5 All data owned, processed or held by the college, whether primary or secondary, must be accessed, stored, transmitted, processed and backed up in a manner appropriate to its security classification.

## 9. Personal Use

9.1 The IT facilities provide by the college are for the use of business-related work or study. However, reasonable personal use is permitted during break or outside normal working hours on the basis that:

9.1.1 it does not interfere with your work or performance

9.1.2 It does not incur a cost for the college.

9.1.3 It does not have a negative impact on the college

9.1.4 it falls in accordance with the rest of this policy

9.1.5 You understand that even though you may be using the device for personal use, this usage may also be monitored in accordance with section 7 of this policy.

9.2 You will not bring in external media with your own content due to the potential risk of viruses and breaches of data protection.

## 10. The Internet and External Platforms

10.1 Copyright applies to all text, pictures, video and sound, including those sent by email or on the internet, intranet / extranet (SharePoint), Moodle (Weblearn) or Google Classroom. Files containing copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

10.2 The use of personal social media accounts must be kept separate from any college accounts. The connections between staff and students using any account that is not authorised or managed by the college is prohibited. Any external facing media content must conform to other college policies. Please see Social Media Policy & Staff Code of Conduct.

10.3 The use of third-party applications is permitted but due diligence must be taken when appointing a service provider from both a financial and technical stand point. All services must be checked to make sure that they are compatible with the college systems and that any data exported is done so to conform to the college Data Protection Policy.

10.4 Internet is provided to the college and externally is seen as one internet connection. No user should use the internet in a way that is illegal, breaches any college policy or breaches the JANET acceptable use policy.

10.5 Any use of the college internet can and will be monitored for safeguarding and security reasons. To use the internet on a personal device and on an approved SSID, you may be required to install a security certificate first. This will allow the inspection of internet traffic on your device.

10.6 You will not download or upload unusually large amounts of data to and from the college IT facilities without prior approval from the Director of IT.

## 11. College Wi-Fi on Personal Devices

11.1 The college will broadcast multiple SSID's but not all are for use for everyone. Some SSID's are reserved for college owned devices and if that is the case, they will have been configured to use the correct one so do not try to change it.
11.2 The only SSID's available to staff, students and visitors are the Eduroam and the Nescot-Guest connections. You are not permitted to try and connect to any other college SSID.
11.3 All staff and students should connect to the Eduroam SSID using their domain credentials.
11.4 The Nescot-Guest network is supplied only for guests of the college from outside the organisation.
11.5 To use the Wi-Fi, you may be asked to install a certificate that enables content filtering. The college reserves the right to refuse access to the internet if the certificate is not installed.
11.6 Guests are required to fill out a form when logging in for identification before using the college Wi-Fi.

## 12. Remote Access

12.1 The college uses some third party hosted applications as well as allows some on site services that can all be accessed outside of the college campus. These services include but are not limited to Office365, Remote Access Portal, Weblearn, GSuite and ProMonitor. Users are permitted to uses their own devices to access these applications, but security protocols must be adhered to.
12.2 All remote workers must ensure that the device they are using is up to date with all security packages within 14 days of release and is running a full and up to date malware protection program.
12.3 All devices being used for remote access must be vendor supported. E.g., the support for Windows XP ended 8/4/2014 so cannot be used to connect to the college IT Facilities.
12.4 Users are not permitted to save any personal or sensitive data from the college on their personal devices.
12.5 You must not leave your computer or device unattended and unlocked whilst connected to any remote service.
12.6 When using Wi-Fi, the user must ensure that the Wi-Fi is secure (requires a passcode to connect).
12.7 Users must ensure that the default passwords for routers and firewalls of the network you are connecting from has been changed from the default and that best security practices are being used.
12.8 Users must refrain from using public Wi-Fi with no security e.g., coffee shops to connect to college services.
12.9 All users must use adhere to all application security protocols and use Multi Factor Authentication where provided.

12.10 Remote access services are only available to approved users.

# Document Control Information:

| | |
|---|---|
| Version | V7 |
| Policy Originator: | Director of IT |
| Equality Impact Assessed: | |
| Approved by: | SMT |
| Date Approved: | 19/10/19 |
| Review Interval: | 3 Years |
| Last Review Date: | March 2021 |
| Next Review Date: | March 2024 |
| Audience: | Public |
| Entered on SP | **18/01/23** |
| | |

# Approval:

| | |
|---|---|
| Author(s): | Director of IT |
| Request By: | |
| Approved By: | SMT |