Northern College

Policy Title	**Information and Communications Technology (ICT) Acceptable Use Policy**
Who does the policy apply to?	All staff, students, volunteers and governors of Northern College, all other contracted staff
Aims	This policy defines what is and is not acceptable use of college ICT equipment, infrastructure and services.
To be read in conjunction with	Data Protection and Information Security policy Safeguarding Adults policy Safeguarding Children and Young People Policy Staff Code of Conduct Staff and Student Disciplinary Procedures Employee and Student Handbooks
Further advice may be sought from	For students – your Tutor or ICT Support team For staff – your line manager or ICT Support team
Review arrangements	This policy will be reviewed every 3 years. This will ensure its continuing relevance and effectiveness. The College may review the policy prior to this date should operational and/or legislative/guidance matters require it. Further details regarding revisions and review cycle can be found at paragraph 13.

Contents

1. Introduction

1.1. All users of ICT are responsible for the security of the systems and the data on them and should not misuse our facilities. As such all users of ICT, must ensure they always adhere to the guidelines in this policy. Should anyone be unclear on the policy or how it affects them whilst studying or working at the college they should speak to their Tutor (for students) or their Line Manager (for staff) or contact the ICT Support team.

1.2. Misuse can include both deliberate acts and inadvertent actions. The repercussions of misuse have the potential to be severe and can cause financial, operation and reputational damage. Examples of potential damage include, but are not limited to, introduction of computer viruses or other malware and ransomware, legal, financial and reputational damage for loss of data and lost productivity and teaching time due to network downtime.

1.3. This policy does not form part of contracts of employment and we reserve the right to amend it at any time.

2. Aim

2.1. This acceptable use policy for ICT equipment, infrastructure, systems and services is designed to protect and safeguard the College, its employees, students and other partners from harm caused by the misuse of our ICT Systems and data.

2.2. To ensure that all users of Northern College's ICT facilities have a clear understanding of what constitutes acceptable and unacceptable use.

2.3. To ensure that college ICT facilities are used in a way that enhances operations and furthers the College mission and objectives.

2.4. To ensure the College is compliant with the Counter-Terrorism and Security Act 2015 (the ACT); Section 26(1).

3. Scope

3.1. This policy applies to all users of ICT facilities (including but not limited to hardware, software, data, network access, third party/cloud services, online services, VR and immersive devices, artificial intelligence or ICT credentials) provided by or arranged by Northern College.

3.2. The policy applies to activities taking place in any location where access to and the use of any of the College's systems and/or equipment takes place, e.g., laptop computers at home; remote access to any of the college's digital and cloud-based systems and/or networked resources. The policy also covers the use of personally owned devices used on the premises and which are connected to any of the College's network. All users will be deemed to be familiar with and bound by this acceptable use policy. A copy of this policy can be found on the College's website. A paper copy can also be made available upon request.

4. Implementation

The College will ensure that:

4.1. Staff are introduced to the ICT Acceptable Use Policy and related procedures and guidelines, e.g., through staff induction, College Management Team meetings, workforce

development training; to enable ongoing dialogue around the acceptable use of Northern College's ICT facilities.

4.2. Staff who are users of Northern College's ICT facilities will receive a level of training appropriate to their role, with appropriate refresher training every 3 years (including cyber security and GDPR training). This is recorded and monitored through the Continuous Professional Development (CPD) process.

4.3. Students commencing their course will be introduced to the ICT Acceptable Use Policy by their tutor. Students will be made aware of the policies location for future reference. This information will be reintroduced to all students on each course. By using the college ICT services including guest Wi-Fi will be deemed as acceptance of this policy.

5. Policy Acceptable Use

5.1. **Acceptable Use overview**

5.1.1 The general principles and conditions of use of both ICT equipment and systems at the College are set out in a guidelines document for staff in Appendix 1 of this policy and for students in Appendix 2. In these appendices the College sets out expectations of what users should and should not do whilst using College systems and equipment.

5.1.2. ICT systems must be treated with care and used only in accordance with their intended purpose.

5.1.3. Equipment must not be used if there is reason to believe that it may not be in safe working order. Any apparent fault with hardware should be reported to ICT Support.

5.1.4. The use of any ICT equipment or your own device using College services for downloading, storage, printing and/or transmission of materials which the College considers to be obscene and/or offensive or of an illegal nature is prohibited. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct as stated in the disciplinary procedures. Access to sites which constitutes criminal activity will be reported to the police as appropriate.

5.1.5. Users must take all reasonable steps to exclude and avoid the spread of malicious software and must co-operate fully with all measures put in place by Northern College to prevent the spread of such software.

5.1.6. Computer programs on the College systems are protected by copyright. The College has the appropriate licenses for all the software on its systems. Users must comply with all their legal obligations concerning copyright and must not copy any software or other data without the prior authorisation from the copyright owner. Such action would be in breach of copyright law.

5.1.7. Authorisation from the copyright owner does not constitute permission to store, execute or download on the College network.

5.1.8. Priority must be given to use of resources for work or educational use.

Personal use must not:

5.1.8.1. Be of a commercial or profit-making nature, including private consultancy, or for any other form of personal financial gain. This includes using the email system or photocopying facilities for advertising items for sale.

5.1.8.2. Be of a nature that competes or conflicts with the College in any way.

5.1.8.3. If users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance from their line manager, personal tutor or the ICT department.

5.2. **Network**

5.2.1. The Northern College provides a high-speed network infrastructure using both wireless and fixed cabling technologies. Whilst the fixed network points on walls may look alike, they differ in configuration. For this reason, any network moves (including connected telephones) must only be carried out by the ICT Department.

5.2.2. The College provides both desktop and laptop computers that have been configured specifically for the tasks that they perform. College owned computers are configured to link directly to security systems, such as Anti-virus systems, that are approved and managed by the College. Users must not, under any circumstances, connect any unauthorised equipment to the College network without first seeking approval from the ICT Department. This does not include the College's guest Wi-Fi network (please see below).

5.2.3. The College provides "guest" Wi-Fi to an unsecure zone on the network; this can be accessed by connecting your device to "NC Guest" and accepting terms and conditions. This is a restricted zone, offering minimal services to users. Permission to connect to this system is not an automatic right and may be withdrawn at any time.

5.3. **Email & Communication systems**

5.3.1. Emails should be drafted with care. Despite their sometimes-informal style, emails are a permanent form of written communication. Users should not make derogatory remarks in emails about employees, students, competitors or any other person. Any such remarks may constitute libel. It is also worth noting that material can be recovered even when it is deleted from your computer.

5.3.2. Users should not facilitate the spread of unsolicited email; you should not respond to "chain letter" style emails that request that a message is forwarded to multiple recipients. This extends to emails purporting to give details of new viruses or "scams". If any user receives such an email and has concerns, they should forward it to the ICT Support team who can check the authenticity of the claims.

5.3.3. Sending email does not guarantee delivery. Delivery receipts do not guarantee that a message has been read. If an email is important, consider asking the recipient to confirm by replying.

5.3.4. Reasonable private use of email is permitted for students but should not interfere with your study. The contents of personal emails must comply with the restrictions set out in the acceptable use policy. Staff should not use their work email account for personal or private use. All emails sent and received by the College system are passed through a third-party virus scanning process and therefore considered safe to open. The College does not sanction the use of web-based email (other than the

College system and College supported systems, such as Office 365) and email received to these systems may not be virus free.

5.3.5. All emails received by the College are filtered in an attempt to remove unsolicited commercial email ("Spam") and phishing attempts to retrieve personal data. Such systems are not fool-proof and individuals should take care when assessing the validity of emails asking for information. More guidance can be sought from the ICT Support team.

5.3.6. The College also provides all ICT account users with access to the Microsoft Teams communication application for use linked to college study or for employee collaboration. As per the acceptable use of email above, whilst Teams is less formal, communications should follow the same protocols. Again, such communications even when deleted can still be retrieved should there be a reason for this to happen, e.g., during an investigation as a result of misconduct.

5.4. **Password Guidelines**

5.4.1. Passwords are an important means of protecting a user's privacy from unauthorised access. With minimal effort, users can greatly increase the effort required by an unauthorised user to compromise information and/or privacy.

The following points relate to password selection and use on all ICT Systems:

5.4.1.1. A password is defined as a secret series of alpha-numeric characters that allow a user to access a computer, program, file or other ICT resource.

5.4.1.2. Passwords should not be shared. Users may receive phone calls from people claiming to be ICT employees asking for a user's password. Users should never give their password to anyone under any circumstances. Users are responsible for all activity on their account.

5.4.1.3. Users should log out of or otherwise lock computers or other resources when finished using them.

5.4.1.4. Passwords should be at least twelve characters long. Passwords should not be the same as a users' logon ID and should not be a word found in a dictionary.

5.4.1.5. Passwords should not be written down in insecure locations. Insecure locations include, but are not limited to, under the system keyboard, system monitor or desk. If a password must be written down, it should be kept in a secure location.

5.4.1.6. Most incidents of computer "hacking" or other forms of uninvited intrusions are the result of poor password selection or protection. ICT personnel may occasionally audit passwords as part of a security exercise. If a password is found that does not meet requirements, the user will be notified and asked to change their password to meet the requirements.

5.5. **Internet**

5.5.1. All internet traffic is monitored logged and recorded.

Do:

5.5.1.1. Only use your own ICT account to access the Internet.

5.5.1.2. Logoff when you have finished using the computer.

5.5.1.3. Lock or log off computers when you are away from your desk.

Don't:

5.5.1.4. Access the Internet from an account other than your own.

5.5.1.5. Download unauthorised or unlicensed software.

5.5.1.6. Access, view or download information, graphics, pictures etc. that are deemed to be defamatory, obscene, racist, sexist or may be of a criminal nature. This could include material that incites racial hatred, condones and encourages support for terrorism and forms of extremism leading to terrorism.

5.5.1.7. Use the Internet to set up or run a personal business.

5.5.2. In the interests of information security, the College restricts access to certain sites and prevents the downloading of certain types of files and content. You must not download, or attempt to download programs, viruses, hacking tools, and copyrighted material. You must not access, or attempt to access, sites which offer or promote such downloads. If you are in any doubt, contact ICT Support.

5.5.3. Any attempt to bypass any filtering or security system may lead to disciplinary action and may be treated by the College as gross misconduct.

5.5.4. If you have a legitimate request to download something that is blocked by one of the College security systems, you should submit a request via email to the ICT Support team who will evaluate the request and take the appropriate action.

5.5.5. The sites accessed by you must comply with the restrictions set out in the acceptable use policy and associated guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. Any access or attempted access to sites deemed to be in breach of the law will be reported to the appropriate authorities.

5.5.6. Reasonable private use of the internet is permitted but should be kept to a minimum and should not interfere with your work or study. For staff, excessive private access to the internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. For students, private access should not occur during taught sessions.

5.5.7. College devices utilising mobile data networks (4G/5G) such as mobile phones, laptops with mobile data capabilities and tablets have limited allocations of data and additional data costs are high so personal use of these devices for internet use should be for exceptional circumstances only.

5.6. **Social Media**

5.6.1. The definition of social media in the context of this policy is as follows: the opportunity to use instantaneous channels for information sharing and communication through social networking opportunities such as Facebook, Twitter, Instagram, TikTok Tumblr, Snapchat and YouTube. Social media can include text, audio, video, images, podcasts and other multimedia communications.

5.6.2. Social media opportunities undoubtedly offer huge advantages in terms of student and staff to interact with each other and enhance communication, teaching, and learning. However, such communication methods can increase the risk of

misinformation, inappropriate communication, unprofessional behaviour, and negative impact.

5.6.3. The College is of the opinion that all information posted on the Internet using social media technologies, should be considered as published, permanent and potentially public, even if it can be deemed as 'protected' in some way. By their very nature, social media technologies are designed to enable quick and simple ways of sharing information and it can be very easy to inadvertently share information to far more people than was originally intended. Seemingly innocent information such as photographs, videos, opinions or comments can be vulnerable to misrepresentation and unauthorised distribution.

5.6.4. All staff and students should think about the reputation of the College. They should think carefully about how they express themselves, and bear in mind the need to safeguard themselves. Material posted on the Internet can be hard to delete and should, therefore be considered permanent.

5.6.5. Default privacy settings on some social media websites allow some information to be shared beyond an individual's contacts. The user is personally responsible for adjusting the privacy settings of the account. Staff and students are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites.

5.6.6. Where students or staff make use of social media and networking technologies (including both internally and externally hosted sites) it is expected that they should not post comments or any other type of material on a social networking site, blog, or send text messages/digital messages that:

5.6.6.1. Could be viewed as bullying or harassing another individual.

5.6.6.2. May be interpreted to be racist, homophobic, sexist, ageist or otherwise discriminatory or breach the college's Equality, Diversity and Inclusion policy.

5.6.6.3. Contains language, sound or video which may cause offense to another member of the College community.

5.6.6.4. Expresses opinions or encourages other members of the College community in the incitement of violence, extremism or to break the law.

5.6.6.5. Are likely to bring the College into disrepute.

5.6.6.6. Publish defamatory and/or false material about the college, students or its employees.

5.6.6.7. Upload, post or forward any content belonging to a third party unless you have that third party's consent.

5.6.7. Any transgression of the above guidelines will be viewed as serious by the College, will be dealt with through the College disciplinary procedures and for students, it may result in a removal of College place. Individuals are personally accountable for

content they publish and may be liable for breaches of this policy. The college reserves the right to refer users to the relevant authority, for example, the police where the breach is considered to constitute illegal activity.

5.6.8. If students (or staff) become aware of or are concerned about any inappropriate comments or material that is posted online, they should draw these to the attention of a member of staff (or their line manager) in order that appropriate investigation and action may be taken.

5.7. **Devices and Equipment**

5.7.1. Devices (e.g., laptop, , smartphone or tablet) issued to you by the College should be looked after as if they were your own. A loss of a device may mean not only the loss of availability of the device and its data but may also lead to the disclosure of sensitive information – such as student assessment data. This loss of confidentiality, and potentially integrity, will often be considered more serious than the loss of the physical asset. In these circumstances the College's Data Protection Policy will be followed.

5.7.2. Where possible data should not be stored on the laptop but rather on the network storage systems provided (primarily Office 365).

5.7.3. Unauthorised access and tampering to a laptop, particularly if there are repeated opportunities for access, may:

5.7.3.1. Lead to continuing (and undetected) compromise of information on the laptop itself.

5.7.3.2. Undermine security measures; intended to protect information on the laptop in the event of loss or theft.

5.7.3.3. Lead to compromise systems to which the laptop is connected, for example, a networked system that is accessed from the laptop.

5.7.4. Security should be applied to off-site equipment taking into account the different risks of working outside the College's premises. Regardless of ownership, the use of any information processing equipment outside the College's premises should be authorised by management. Security risks, e.g., of damage, theft or eavesdropping, may vary considerably between locations and should be considered in determining the most appropriate controls.

5.7.5. Ensure that laptops or mobile devices are not left unattended when working off-site. When travelling and not in use, ensure that laptops are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Laptops left on display and unattended will inevitably attract attention and are likely to be stolen. It is good practice to carry laptops in protective anonymous bags or cases (i.e., those without manufacturer logos on them) when not in use.

5.7.6. Do not leave College laptops or mobile devices unattended in car boots overnight. Do not leave laptops unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available.

5.7.7. Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc. and on public transport e.g., buses and trains. When travelling, avoid placing laptops in

locations where they could be easily forgotten or left behind e.g., overhead racks and taxi boots. Be aware that the use of laptops in public places will likely draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

5.8 The Prevent Duty

5.8.1 Northern College understands its duties and obligations within the auspices of The Counter Terrorism & Security Act (2015). The College will ensure that staff, and students are aware of the risks and will monitor them effectively by:

- Ensuring plans are in place to respond appropriately to a threat or incident
- Having effective ICT security, forensic monitoring of IT traffic and ensure that
- the responsibility within the Filtering and Monitoring Standards 2023 are met.Reduce permissive environments by responding appropriately to a locally derived threats or incidents alongside national or international concerns.
- Ensuring students and staff are aware of permissive environments through training and development.

6. Privacy and monitoring

6.1. The College reserves the right to monitor all electronic and voice communication to prevent criminal activity and to detect misuse of college facilities.

6.2. All internet access is logged and contains the username, website location, time, and date. These logs are stored, and reports are routinely generated to review bandwidth usage and check security issues. The College's web-filtering software monitors all websites visited by users for safeguarding, business and security purposes. Therefore, individuals should have no expectation of privacy when it comes to sites they access whilst using college ICT equipment or the College network.

6.3. In addition to the routine reporting, individual managers may, ask for a report on the usage of their staff or students where there is reason to suspect that ICT facilities are being used inappropriately or to prevent criminal activity. Where staff are affected, managers should contact HR for support.

6.4. The content of email communications is not routinely monitored by members of the ICT Services team. However, the ICT Support team have access to all ICT user accounts and the College reserves the right to monitor email communications to support operational, maintenance, auditing, security, and undertake investigative activities. As part of this monitoring activity it may on occasion be necessary to access users accounts in response to a specific need and for the purposes of our legitimate interests,. For staff, access to check an account should be agreed through HR, this may include access to email and would be for the following business reasons:

6.4.1. Employees are absent from work and communications need to be checked to ensure business continuity;

6.4.2. To conduct an investigation into viewing or sending inappropriate content; excessive personal use; a breach of this policy; or suspected criminal activity.

6.5. All College laptops and Personal Computers (PCs) have technology to scan for potentially inappropriate typed or dictated activities and these are automatically flagged for review.

6.6. Telephone communications are not routinely monitored. However, the College reserves the right to do so to support investigative activities. The College has capability to record telephone communications at a system level, also certain systems may have such features to record conversations for staff protection and training purposes (such as Microsoft Teams) –systems will incorporate a notice to inform both parties of such recording.

6.7. Any information obtained through monitoring may be shared internally, including with members of the HR team, your line manager, with the members of the College Leadership Team and IT staff if access to the data is necessary for performance of their roles. However, information would normally be shared in this way only if we have reasonable grounds to believe that there has been a breach of the rules set out in this policy.

7. Artificial Intelligence

7.1 AI is a useful tool to enhance education, support users in their daily tasks, and create an inclusive learning environment. It is recognised that AI is a fast-moving technology, and this information will be regularly reviewed and updated as and when required.

7.2 The following applies to all users of AI technology such as Microsoft Copilot that is used for northern college purposes (such as student or staff work) or on the college network or device.

- All information used on AI platforms should be in compliance with the colleges data protection and data privacy policies.
- Users should remain mindful that all information such as search terms and documents created within AI tools are in the public domain and personal, identifying or sensitive information relating to yourself, the college or other individuals should not be entered into AI platforms.
- Users are prohibited from using AI to create and/or distribute content that is discriminatory, harmful, offensive, or intentionally biased. Where this type of use is suspected the college disciplinary procedures will be followed.
- AI must not be used in assessments unless it is explicitly permitted, this includes but is not limited to:
    - Copying or paraphrasing sections of AI-generated content to the point that the work can no longer be considered to be the users own.
    - Failing to acknowledge use of AI tools when they have been used as a source of information

7.3 We reserve the right to use AI plagiarism detectors or our academic judgement to identify unacknowledged uses of AI.

8. Account management

8.1 For employees and contractors accounts, these will be disabled immediately on ceasing of employment or contract. Based on role the account will be closed in due course. Any work undertaken and saved on College services or systems remains the intellectual property of Northern College.

8.2 For students, the account will be disabled 30 days after the official course end date or when appropriate if an account access extension has been requested by the tutor. It is the student's responsibility to ensure that they take a copy of any work belonging to them.

9. Reporting Incidents

9.1. The College will investigate all security incidents. It is the responsibility of staff and students to report any such incidents in accordance with the information in this policy.

A security breach is:

9.2.1 Any action that results in or potentially could result in the loss or damage to College assets and data.

9.2.2 The unauthorised access to or disclosure of data and information.

9.3.3 Any lapse in security.

10 Responsibilities

10.1 It is the responsibility of all users to read, understand, and adhere to the ICT Acceptable User Policy; to maintain an awareness of current online safety guidance; to understand the importance of reporting abuse, misuse or access to inappropriate materials to the ICT Support Team or Safeguarding team where relevant.

10.2 Security and IT incidents should be reported to the ICT Management who will undertake an initial investigation, log the incident and report to the Deputy Principal and Chief Finance Officer who will then gauge the scale of the incident and decide on further action, briefing the Executive Leadership Team (ELT) where appropriate.

10.3 The Deputy Principal and Chief Finance Officer has executive responsibility for information security. They will maintain overall responsibility for determining appropriate sanctions, reporting on security incidents to the College's Executive Leadership Team and reviewing the effectiveness of the ICT Acceptable User Policy. Specific security tasks may be delegated to certain staff.

10.4 The AP Student Experience has executive responsibility for the safeguarding of students and the Head of HR has the responsibility for safeguarding staff. Monitoring and filtering systems are in place and are facilitated and administered by the ICT Support Team.

11 Monitoring and Evaluation

Policy will be reviewed considering every reported incident. Each year the log of security incidents will be investigated to determine the effectiveness of the ICT Acceptable User Policy. Furthermore, given the fast-changing digital landscape and the ever-evolving threat of a Cyber-Attack, the policy will be reviewed annually. This review will take place between the Deputy Principal and Chief Finance Officer, Head of MIS & ICT and Data Protection Officer (DPO). Subsequent recommendations will be taken to the College Executive Management Team and changes to the ICT User Policy will be directed to the appropriate College committee structures.

12 Sanctions

12.1 All users are hereby advised that violation of one or more of the above conditions of use and/or violations of the related policies shall be treated as a breach of this policy and may lead to disciplinary action.

12.2 Where abuse of the College's ICT systems is identified, such facilities will be withdrawn from the user concerned and disciplinary action may be taken.

13. Policy sign off and ownership details.

Document Name:	NC ICT Acceptable User Policy
Version Number:	V1
Effective from:	April 2025
Next scheduled review date:	April 2028
Policy owner:	Head of MIS and ICT
Approved by:	Audit Committee and Governors

13 Revision history

Version No	Effective date	Revision description/summary of changes	Author
V2	April 2025	This policy replaced the Northern College ICT User Policy – June 2021 . Summary of changes • Job roles updated in line with current organisational structure. • Section 7, Artificial Intelligence (AI) added • Content revised in section 3.1, 5.2.1, 5.5.4, 5.6.1, 5.7.1, 8.1	Head of MIS and ICT

Appendix 1:

ICT Acceptable User Policy – Staff Guidelines

General Principles

- College provided internet, intranet and email services are considered College resources and as such usage may be monitored for unusual activity.
- Correspondence via email cannot be guaranteed to be private. Any confidential email should be sent using encryption techniques sanctioned by the College.
- Use of internet, intranet, email and Office 365 services 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.
- 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.

Reasonable personal use of the internet is permitted but is subject to the terms laid out below and the operational requirements of the College. Personal use of ICT facilities should take place outside of normal contracted working hours (i.e. lunchtime or breaks) and it should not incur an unreasonable cost to the college. The acceptable use policy and conditions of use apply for all access to college systems and services whether accessed on campus, remotely and irrespective of the device used.

Conditions of Use: Users shall not:

- Visit or attempt to visit internet sites that contain obscene, hateful or other objectionable materials; send or receive by electronic means material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Use College facilities to solicit non-College business for personal gain or profit.
- Use the internet, email, telephone system or service for any illegal purpose.
- Represent opinions as those of the College without express consent.
- Make or post indecent remarks, proposals or materials.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging either to parties outside of the College or to the College itself.
- Install or run any unauthorised software on college equipment.
- 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.
- Use Internet, email, telephone or Office 365 services for inappropriate personal use that is not connected with college business.
- Reveal or publicise any confidential or proprietary information which includes, but is not limited to:
    - financial information
    - new business ideas
    - marketing strategies
    - plans
    - databases and information contained therein.
    - student enrolment details
    - business relationships

- Examine, change, or use another users' files, output, or username for which they do not have explicit authorisation.
- Reveal individual passwords, either account logon or system specific, to anyone else.
- Resell any service provided by the College, including but not limited to email, network storage and internet access.
- Enter personal, identifying or sensitive information relating to yourself, the college or other individuals into AI platforms. Use AI algorithms to create convincing forgeries of individuals' likenesses, known as deepfakes. A zero tolerance approach will be taken to the generation of deepfakes and presentation of these as authentic content and users will be referred to the college's disciplinary procedures.

Social media

- The college encourages the positive use of social media as part of the educational process.
- When using social media in any capacity, employees actions can still damage the college's reputation so employees should conduct themselves accordingly.
- Staff must not use their work email address to sign up for personal social media websites.
- Staff should have no expectation of privacy or confidentiality in anything they create or share on social media platforms. When you create or exchange content using social media you are making a public statement. As such, your content will not be private and can be forwarded to third parties without your consent. Staff should therefore consider the potential sensitivity of disclosing information (such as health information). Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered and this may result in liability both for the College and also you personally. Bear in mind that, even if you are using social media in a personal capacity, other users who are aware of your association with us might reasonably think that you speak on the College's behalf. Staff should also bear in mind at all times any adverse impact your content might have on our reputation or supplier relationships.

In addition to the points set out in section 5.6 staff should:

- Limit their personal use of social media to break times or times when they are not on duty (i.e. before or after work). The limits on personal use also apply to time spent on social media on employees own devices including for example, laptops or smartphones. Excessive use of social media which interferes with work duties and responsibilities will be considered a disciplinary issue.
- Be mindful of the boundaries between professional and personal life. If expressing personal views it should be clear that these are personal and not the views of the college.
- Only set up a professional account with consent from a member of ELT.
- Staff or students should not be referenced (tagged) online without their express consent.
- Not breach confidentiality by disclosing privileged, sensitive and/or confidential information.
- Check that a third party website permits you to link to it before including a link and ensure that the link makes clear to the user that the link will take them to the third party's site.
- When linking to college accounts, not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip and not escalate 'heated' discussions. Try to be conciliatory and respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset; return to it later when you can contribute in a calm and rational manner.
- Participate in activity which may compromise an employees position at the college.

- Be honest and open but also be mindful of the impact your contribution to a site may have on the perception of the College.
- Admit if they make a mistake in a contribution, be prompt in admitting and correcting it.

Acceptance of friends

Social media is used by many people, particularly students to communicate with their peers and the public. Students may wish to form personal relationships with employees, however to ensure professional boundaries are maintained, you must not accept and/or invite the following individuals to be 'friends' on personal social media accounts or other online services:

- Students of any age,
- ex-students under the age of 18, and
- parents

Entering into such relationships may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected by us. The College reserves the right to take disciplinary action if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.

Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Children Board (LSCB) and/or the Independent Safeguarding Authority (ISA).

Use of social media during recruitment and selection process

The College may view relevant social media websites as part of the pre-employment process, i.e. those aimed specifically at the professional market and used for networking and career development (e.g. LinkedIn). Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

Inappropriate conduct on social media

Employees should note, in particular, that creating or sharing content on a social media platform may amount to misconduct even if it takes place:

- on a personal account with appropriate privacy settings;
- outside normal working hours; and/or
- without using our computers, systems and networks.

Members of staff who violate any of the guidelines set in the policy may be subject to disciplinary action. The College also retains the right to report any suspected illegal activities to the appropriate authorities. Further guidance can be found in the full IT Acceptable Use Policy document. If there are any queries relating to this document, please contact the ICT department.

Appendix 2:

ICT Acceptable User Policy – Student Guidelines

General Principles

- College provided internet, intranet, email and Office 365 services are considered College resources and as such usage may be monitored for unusual activity.
- Correspondence via email or Microsoft Teams cannot be guaranteed to be private.
- Use of internet, intranet, email and Office 365 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.
- The distribution of any information through the internet, computer-based services, email and Office 365 systems is subject to scrutiny. The College reserves the right to determine the suitability of this information.
- Reasonable personal use of the internet and email services is permitted but is subject to the terms laid out below and the operational requirements of the College.
- The acceptable use policy and conditions of use apply for all access to college systems and services whether accessed on campus, remotely and irrespective of the device used.

Conditions of Use: Users shall not:

- Visit or attempt to visit internet sites that contain obscene, hateful or other objectionable materials; send or receive by electronic means material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Use the internet, email, telephone systems or other College systems for any illegal purpose.
- Represent opinions as those of the College without express consent.
- Make or post indecent remarks, proposals or materials.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging either to parties outside of the College or to the College itself.
- Install or run any unauthorised software on college equipment.
- 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.
- Use Internet, email or telephone services for inappropriate personal use that is not connected with teaching and learning.
- Examine, change or use another users' files, output or username for which they do not have explicit authorisation.
- Reveal individual passwords, either account logon or system specific, to anyone else.
- Resell any service provided by the College, including but not limited to email, network storage and internet access.
- Use AI algorithms to create convincing forgeries of individuals' likenesses, known as deepfakes. A zero tolerance approach will be taken to the generation of deepfakes and presentation of these as authentic content and users will be referred to the college's disciplinary procedures.

Students who violate any of the guidelines set in the policy may be subject to disciplinary action. The College also retains the right to report any suspected illegal activities to the appropriate authorities. Further guidance can be found in the full IT Acceptable Use Policy document. If there are any queries relating to this document, please contact the ICT department.