# IT Usage Policy

Review

| | | | |
|---|---|---|---|
| Formal Review Cycle | 36 months | | |
| Latest Formal Review (date) | 21/07/2020 | Next Formal Review Due (date) | 21/07/2023 |
| Policy Owner | Group Director of ICT and Learning Innovation | | |
| Policy Author | Scott Clennell – Group Director of ICT and Learning Innovation | | |

Approvals

| | | | | | |
|---|---|---|---|---|---|
| Board of Corp Y/N | | Committee | | Date Board approved | |
| SLT Y/N | Y | SLT date approved | 28 July 2020 | Additional committee | |

Publication

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Website Y/N | N | Intranet Y/N | Y | Student VLE Y/N | Y | Other | |

Change History

| Version | Date Reviewed/ Revised | Description of Change | Reviewed by | Approved by |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# IT Usage Policy

## 1. Policy Statement

**1.1.** This policy is a policy of the City of Sunderland College, trading as Education Partnership North East (which includes Sunderland College, Hartlepool Sixth Form College and Northumberland College). These colleges will be referred to as "the College" throughout this document.

**1.2.** Safe use of IT systems, equipment and cyber security is the responsibility of everyone, with every user making decisions about how they access and store their own data, and how they behave when interacting with computer-based systems and networks.

**1.3.** Enable all users (staff, students, and others) of College IT equipment or systems to use these systems safely and securely and informs users of their responsibilities and College expectations for appropriate use of these systems.

**1.4.** Ensure that all users are aware of what the College monitors in terms of usage, and any actions that may be taken if the policy is breached.

**1.5.** This does not form part of any contract of employment or student agreement put in place and may be amended at any time to ensure fitness for purpose against emerging changes.

## 2. Scope

**2.1.** All users of College systems. This includes, but is not limited to, all members of staff, all students, governors, visitors, contractors, and affiliates.

**2.2.** All usage of College systems and equipment, whether this be in College locations or at other locations.

**2.3.** All usage of these systems, including access away from College or in College on equipment not owned by the College.

**2.4.** All systems and technical equipment are in scope. Appendix 1 lists the main areas of systems and equipment.

## 3. Aims of the Policy/Underpinning Principles

There are 6 key aims of this policy:

**3.1. Provide a Safe and Secure digital College**

3.1.1. The College and all users of College systems have a responsibility to ensure and promote safe and secure usage of IT systems. This is to ensure that our students are protected and appropriately safeguarded from online threats of various forms, whilst encouraging digital safety and developing digital citizens with strong and employment ready digital skills.

3.1.2. Ensure the safety of data and information from unauthorised access, to maintain strong compliance with Data Protection Regulations and protect the reputation of the College as a safe custodian of personal and other sensitive data.

3.1.3. Ensure that all users of College systems are proactively protected from safeguarding risks, and radical/extremist/extremist group content.

**3.2. Embed positive use of systems for all and ensure a positive College reputation**

3.2.1. Set clear guidelines of acceptable system use to ensure positive impact on staff and students, and to promote a strong College reputation.

**3.3. Enable greater agility and effectiveness for our users**

3.3.1. We recognise the rapidly changing expectations of all users of our systems, and this policy seeks to enable the agility and greater effectiveness and impact these changes can have, whilst always maintaining the other clear principles of the policy.

**3.4. Ensure Accessible and Inclusive provision for all**

3.4.1. The College is passionate and proactive in ensuring equal opportunities for all, regardless of their background. This policy aims to ensure that our IT systems are used positively to promote this inclusivity and prevents the exclusion of any individuals or groups.

3.4.2. As well as ensuring access to systems is not used to discriminate, the College also encourages the use of assistive technologies available to staff and students as much as possible. These technologies include assistance with screen reading, translation, speech to text, amongst many others. (See sections 5.4.5-6 below).

**3.5. Ensure Reliability and Continuity of our services**

3.5.1. Ensure that the reliability and continuity of IT systems is always maintained as much as possible, and the usage outlined within this policy seeks to prevent "risky" activity on College systems that could otherwise lead to degraded services for other users.

**3.6. Protection from Financial or Compliance risks**

3.6.1. Reduce preventable financial or compliance impact to the College through positive and respectful use of all College systems.

3.6.2. This will ensure compliance with relevant legislation around the use of IT systems and equipment, including but not limited to GDPR regulations, Equality Act, and the Computer Misuse Act. Therefore, the likelihood of a breach in these legislations, or a data breach event, will be significantly reduced, ensuring the ongoing financial and reputational positions of the College.

**3.7. Equality and Diversity -** The College values diversity and inclusion and is committed to promoting equal opportunities and eliminating discrimination. Therefore, staff will apply and administer this policy fairly and consistently to ensure that there is no discrimination on the grounds of age, disability, gender reassignment, marital and civil partnership status, pregnancy and maternity, race, religion or belief, sex, sexual orientation, (and for student facing policies include) young persons in care and care leavers, young carers and care givers, young parents, youth offenders, and those receiving free school meals.

## 4. Responsibilities

**4.1.** It is the responsibility of **all users of College systems** to review, agree to, and ensure their personal compliance with this policy.

**4.2.** The Group Director of IT is responsible for ensuring:

4.2.1. The ongoing relevance and review of this policy.

4.2.2. Communication of this policy to all leaders within the College.

4.2.3. Ongoing monitoring of policy compliance.

**4.3.** All **Leaders** in the College (defined as anyone with line management responsibility), are responsible for:

4.3.1. Ensuring this policy is communicated to all staff within their departments in a timely fashion (within 4 weeks of amendment or release).

4.3.2. Proactively ensuring that team members sign up to the policy and monitor ongoing compliance within their teams.

4.3.3. Instigate investigation and/or other processes, or support these processes, if a breach or suspected breach is highlighted.

**4.4.** All staff in the College whose role leads to external stakeholders receiving College system access of any form (e.g. Governors, Contractors, on site Visitors) are responsible for ensuring the steps outlined in 4.3 above are followed for these users.

**4.5.** The Director of Student Services is responsible for ensuring this policy is communicated to all learners in the College.

**4.6.** All curriculum/teaching staff are responsible for ensuring that the steps outlined in 4.3 are followed for learners in their respective areas.

**4.7.** The Group Director of People and Development is responsible for ensuring the investigation of, and any subsequent action taken in regard to, any breaches or suspected breaches of this policy.

## 5. Implementation

### 5.1. Acceptable Use

**5.1.1.** All users of College systems will be asked to read and agree to this policy prior to being given access to these systems and asked to review this at the time of any changes to this policy.

**5.1.2.** All users must always access within the guidance outlined by this policy.

**5.1.3.** Systems must not be used for any form of unacceptable use. Broadly, this includes any activity that is, or could be viewed as, leading to any of the following:

**5.1.3.1.** Access or usage not in line with British Values.

**5.1.3.2.** Risks to staff, students, or other users of College systems. This includes but is not limited to:

**5.1.3.2.1.** Any usage of systems to access or share content that could be related to extremism, extremist groups, or terrorism, in line with the College PREVENT duty.

**5.1.3.2.2.** Any usage of systems to access or share content that could be deemed to cause risk or harm to learners, in line with the College Safeguarding Policy.

**5.1.3.3.** Impact on College systems, or on College reputation.

**5.1.3.4.** Inappropriate communication – including offensive, discriminatory, defamatory, or otherwise unprofessional.

**5.1.3.5.** Illegal or immoral activity.

**5.1.3.6.** Impact to the College's ability to comply with the law or other regulations, including Data Protection and licensing compliance.

**5.1.3.7.** Impact to the College financially.

**5.1.3.8.** Breaches of any other College policies – including but not limited to Dignity at Work, Equality, Diversity and Inclusion Policy

**5.1.4.** A non-exhaustive list of examples of unacceptable usage of systems includes:

**5.1.4.1.** Attempting access to or distribution of pornographic, obscene, or indecent materials, or any content which could be regarded as explicit or sexual in nature.

**5.1.4.2.** Attempting access to or distribution of any illegal content, including access to any extremist materials, or materials from extremist groups, which promote terrorism, terrorist ideologies, violence, or intolerance, or could otherwise support radicalisation.

**5.1.4.3.** Attempting access to or distribution of any other content that could be viewed as offensive by another person.

**5.1.4.4.** Attempting access to or distribution of content relating to illegal activities, including drug and substance abuse, hacking/malware, and violent acts.

**5.1.4.5.** Attempting access to or distribution of content which is "pirated" – i.e. copyright theft. This includes access to any "peer to peer" networks, Usenet/Newsgroups, and any other related technologies.

**5.1.4.6.** The sending of email or other communication that has the potential to cause offence or anxiety to the recipient or would otherwise not be treating the recipient with the respect and dignity deserved, or that could promote the unjust and prejudicial treatment of people on the grounds of protected characteristics (as listed in the Equality Act 2010).

**5.1.4.7.** The use of College systems for any commercial activity outside of College interests.

**5.1.4.8.** Any attempt to circumvent College security and safety systems, such as web filtering and password stores. This includes the usage of any systems which could be used to attempt to circumvent these, such as TOR networks, VPN usage, and proxy/filter bypass technologies.

**5.1.4.9.** Any use of College systems that could lead to damage to the College's reputation or show the College in an unprofessional light, whether this usage is intended to be public or not.

**5.1.4.10.** The sharing of usernames, passwords, or any other security details with others, including the storage of these details insecurely.

**5.1.4.11.** Access to or sharing of any data, including personal data or commercially sensitive data, inappropriately inside or outside of the College.

**5.1.4.12.** Not taking appropriate care of any College IT assets, or intentionally causing damage to these assets.

**5.1.4.13.** Any activity (intentional or otherwise) that could cause impact on performance or accessibility to College systems (for example, excessive usage of wireless for non-College purposes, or the automation of multiple accesses to College systems).

**5.1.4.14.** The purchase, usage or installation of any new software, hardware, or internet service without prior authorisation of the IT department.

**5.1.4.15.** Storing data on any device not authorised by IT. This includes the usage of personal/unencrypted USB or other removable storage. Encrypted USBs may be used where issued by IT, but users are encouraged to instead utilise College platforms (OneDrive, Teams and SharePoint) to allow access to data.

**5.1.5.** Users of College systems are permitted to use systems for personal use. However, this usage must still be in line with the policy and acceptable usage above. Any online communication of a personal nature must not breach this policy, and it should be made clear to the recipient(s) that any such communication is personal in nature.

**5.1.6.** Note that due to the rapid pace of change in digital technologies and content, this policy is not designed to be exhaustive in defining "inappropriate use". Instead, the general principles within 5.1.3 should always be adhered to, and clarity sought through the College leadership team or IT if there is any doubt as to the appropriateness of a particular use of College systems.

## 5.2. Devices and equipment

**5.2.1.** In addition to the Acceptable Usage outlined in 5.1, there is specific policy guidance on the use of IT devices and equipment as outlined below.

### College Owned Equipment

**5.2.2.** College owned equipment should never be used other than for its intended purpose and no modifications should be attempted – for example, College owned equipment should not be dismantled, damaged, or used for any other purpose than access to services.

**5.2.3.** College owned equipment must not be taken off College premises unless previously agreed by IT (for example, laptops and phones issued to staff).

**5.2.4.** College owned equipment that is loaned to any user must be returned to IT by the time and date agreed with IT at the time of loan. This equipment should never be passed to another user.

**5.2.5.** Should any equipment be damaged, or observed to be damaged, due to any reason, this should be immediately reported to the IT Service Desk so that this can be rectified, and service maintained.

**5.2.6.** Anyone using College equipment outside of College premises is always expected to treat this equipment respectfully and ensure its security and integrity. When not in use this equipment must be stored securely (for example, not left in a car boot or other potentially insecure location).

**5.2.7.** We understand that issues can occur with equipment especially away from College premises. Should equipment be damaged, lost or stolen at any time, this should be immediately informed to the IT Service Desk to ensure that we can protect any information and data stored on it, and to attempt to retrieve or repair the equipment.

**5.2.8.** Whilst College owned equipment may be allocated to individuals or departments for operational reasons, the equipment remains under the control and ownership of the IT Directorate and these devices may be withdrawn or redeployed at any time should the needs of the College require it. On request any equipment must be returned to IT expediently.

**Personal Owned Equipment**

**5.2.9.** The College permits, and indeed encourages, the use of personal devices to access College systems, be this when on campus or away from campus. However, there are some special considerations for this usage.

**5.2.10.** To ensure such access is compliant with this policy and other College policies, you may be required to permit some limited access to the personal device to allow for management of applications and monitoring. The full details of this management will be provided for consent at the time of such access, and this consent may be withdrawn at any time. This access would never exceed that required to ensure compliance with this policy. However, the College reserves the right to prevent personal device access to systems should this consent not be in place.

**5.2.11.** Users should take particular care when bringing a personal device on campus to ensure that no applications or software is installed or running (actively or in the background) prior to connecting to College systems. For example, any web pages open on a mobile device in the background which would be in breach of this policy must be closed prior to bringing the device on campus.

**5.2.12.** The College can accept no responsibility for any damage that may be caused to this device at the time of this usage – for example, virus infection, power surge damage, accidental damage, etc.

**5.2.13.** The College also cannot support personal devices and technical support for these will be limited. The College would always seek to provide guidance where possible to allow for the use of these devices.

**5.2.14.** Any College data must never be stored on personal devices under any circumstance, except where this occurs through a managed application (as per 5.2.10). For example, documents should not be saved locally but instead only to the College maintained storage platforms.

**5.2.15.** Within areas where students or staff access College systems outside of College hours and for personal reasons (e.g. halls of residence, on site duty head), the College encourages the usage of internet and other IT platforms in order to be able to have access to information and relaxation when residing on College premises. For these users, internet filtering may be relaxed to permit greater recreational use – for example usage of streaming media, and access to games sites etc. However, this usage is still within the remit of this policy and be aware that this usage is still monitored and enforceable if required (as per section 5.5 of this policy).

**5.2.16.** The use of personal devices in any form, and/or the use of College systems for personal usage, is a non-contractual benefit provided to users. Should the College deem it necessary for College reasons this usage can be withdrawn, either on individual cases or collectively, at any time and without notice.

**Storage Devices (USB Drives/External Drives)**

**5.2.17.** As per sections 5.2.14 and 5.1.4.15 above, external drives of any form should not be used to store College data. Instead, staff and students should utilise the storage platforms made available to them to access data when away from College locations.

**5.2.18.** This includes external hard drives, USB “pen drives”, and any other device capable of transferring data to and from a computer.

**5.2.19.** The only circumstances in which such an external drive should be used is if the drive is one provided by the College IT department, which are encrypted to prevent data loss.

**5.2.20.** However, we would still encourage all College users to use the College storage platforms unless the location the data needs to be accessed is unlikely to have internet access permitting access to these platforms.

### 5.3. Security

**5.3.1.** All users will be given access to systems in a secure fashion, using various security techniques, most commonly to end users as a username and password.

**5.3.2.** These details should be treated with the utmost confidentiality and must never be shared with anyone other than yourself (including any request from IT or senior leadership – these details would never be requested). These details should be treated with the same level of protection as would be given to physical keys to a building or house.

**5.3.3.** Any breach of 5.3.2 is a serious breach of this policy and would result in the individual being responsible not only for this breach, but also any subsequent breaches of this policy or College systems resulting from this.

**5.3.4.** Password and other security policies may change over time in line with best practice provided by the NCSC (National Cyber Security Centre) and such changes will be informed to all users. No users will be permitted, nor should it be requested, to have a "softening" or removal of these policies.

**5.3.5.** User devices must never be handed over to other users, left logged in and unlocked when unattended, or otherwise be put in a position to be compromised.

**5.3.6.** Unsolicited emails or other communications, especially those containing links or attachments, should not be opened. If there is any doubt as to the legitimacy of such a communication this should be raised to the IT Service Desk prior to opening.

**5.3.7.** Some systems may require "Multi Factor Authentication" (MFA), in the form of a username and password, but also another form of authentication – most commonly a passcode sent to a mobile phone. If a user has this access, the loss of the device on which this is received whether personal or College owned, should be reported to the IT Service Desk immediately to ensure appropriate protection to College systems.

**5.3.8.** Given the close relationship between IT usage, cyber security, and data privacy, the College reserves the right to withdraw IT system access for any users who have not performed cyber security and data privacy training within the preceding 3 years.

### 5.4. New Software/Services/Other Technology Requirements

**5.4.1.** All requests for any new software, service, or other technology should in the first instance be put to the IT Service Desk.

**5.4.2.** Such requirements will be assessed via an Impact Assessment, in conjunction with the requestor, to ensure that the request is:

- **5.4.2.1.** In line with IT Strategy and Policy
- **5.4.2.2.** Has a clear business case and need
- **5.4.2.3.** Is fully costed, including support and future costs, in line with this business case
- **5.4.2.4.** Compliant with Equality Impact Assessments
- **5.4.2.5.** Compliant with Data Protection Impact Assessments
- **5.4.2.6.** Compliant with licensing regulations

**5.4.3.** Users must not sign up or use any such service, nor put any data within the remit of such a service, without this process being completed. This is to ensure the protection of the College's legal compliance, alignment to organisational goals, and financial and reputational positions.

**5.4.4.** The entirety of section 5.4 includes "free" software, any cloud/web-based services, any devices that require connectivity to College systems, and any software or service that may be used elsewhere in the College. This also includes the use of any of these services on personal devices for the purpose of College activities.

**5.4.5.** Staff should seek to proactively understand any challenges that either their direct reports, or, in the case of curriculum staff, their learners have regarding the usage of College systems. These

challenges should be raised to the IT department so that the College can provide assistive technologies as appropriate to support this to ensure staff and students are not disadvantaged.

**5.4.6.** Should learners be recognised to be disadvantaged due to a lack of digital equipment availability outside of the College premises, again this should be raised to the IT department at the earliest opportunity so that we can provide potential solutions to support these learners.

**5.5. Filtering and Monitoring**

**5.5.1.** All users should be aware that all usage by all users of College systems is monitored and logged against the user.

**5.5.2.** In addition to monitoring of usage, filtering of inappropriate or potentially inappropriate access is explicitly filtered. This filtering is in line with best practice guidance, such as those provided by the UK Safer Internet Centre.

**5.5.3.** Any users accessing, or attempting to access, inappropriate materials will be recorded, and investigations will be commenced where there is reasonable suspicion of a breach of this or any other College policy as a result.

**5.5.4.** Should any users feel that material is being filtered incorrectly, or otherwise could impact upon learning activities, a request should be made to the IT Service Desk who will assess any potential change. Any changes will be made on a case by case basis.

**5.5.5.** All users should be aware that filtering changes on a near daily basis and as such changes may be made to filtering without notice. It is important therefore that users do **not** assume that content not blocked is safe or within policy, access to material should be based on the guidance outlined in this document.

**5.5.6.** The College proactively monitors on a regular basis (minimally daily) any access to content through College systems that is, or could be, in breach of this policy, or could otherwise affect the safeguarding and e-safety of our learners.

**5.5.7.** It is the responsibility of **all staff and students** in the College to report to the IT team any observed breach, or potential breach, of this policy, and/or any observed usage of systems that may constitute a safeguarding concern.

**5.5.8.** In the event of an issue being highlighted through proactive monitoring or reactive reporting, this will be passed to the appropriate member of College staff to assess and if necessary appropriate disciplinary action being taken against the user.

**5.5.9.** The College may access any College stored data, including that within the area of an individual (such as e-mail, internet history, etc), if it needs to do so for the purposes of legal obligations or the protection of the College. There should be no expectation of privacy for users when using College systems.

**5.5.10.** Any usage of systems that constitutes a breach of legislation, or any criminal laws, may result in that individual also having action taken against them by the appropriate body.

**5.5.11.** The College treats the privacy and security of its information and systems with the utmost importance, and serious breaches of this policy could constitute a gross misconduct issue (in the case of staff) or a student being ruled as unable to return to the College.

## 6. Policy Communication and Training

**6.1.** To ensure awareness and compliance with this policy, all staff and students will be expected to review this policy and explicitly agree their understanding at induction, and subsequently every 12 months.

**6.2.** Should this policy be revised, all staff and students will be informed of this change and required to confirm their understanding and agreement with the revised policy.

**6.3.** Should either 6.1 or 6.2 not be adhered to, to ensure policy compliance access to College systems may be revoked to individuals until such point that this agreement is completed.

**6.4.** In order to support awareness and communication of this policy, and to ensure understanding, this will be supplemented by mandatory training packages for staff and students to complete when providing

their agreement to the policy, which cover the key points outlined and support users to stay compliant and safe when using College systems.

**6.5.** In the case of users of College systems who are not staff or students (for example, visitors to campus), these users will be asked to confirm their agreement to this policy prior to any access. Staff responsible for visitors should be aware that this access will not be granted prior to acceptance of the policy.

## 7. Associated Documents

This policy relates closely to, and is aimed to support compliance with, the following regulations, policies, and guidance:

**College Policies**

- Safeguarding Policy
- Dignity at Work Policy
- Data Protection Policy
- E-Safety Policy
- Equality, Diversity and Inclusion Policy
- Anti-Bullying Policy
- Social Media Policy
- Staff Code of Conduct
- Student Disciplinary Policy
- Student Code of Conduct
- Induction Policy
- Disciplinary Policy

**Legislation**

- Counter-Terrorism and Security Act 2015
- Equality Act 2010
- Computer Misuse Act 1990
- Data Protection Act 2018 (General Data Protection Regulation)
- Obscene Publications Act 1959
- Protection of Children Act 1999
- Criminal Justice and Public Order Act 1994
- Race Relations Act 2000
- Public Order Act 1986
- Equal Opportunity Act 2010
- Defamation Act 2013
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Education Act 2002
- Children Act 2004

**Guidance**

- Keeping Children Safe in Education - https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- UK Safer Internet Centre - https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring
- NCSC (National Cyber Security Centre) - https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- Prevent Duty - https://www.gov.uk/government/publications/prevent-duty-guidance/prevent-duty-guidance-for-further-education-institutions-in-england-and-wales

## 8. Policy Monitoring and Review

**8.1.** Every 36 months. However, in line with the rapid pace of change within digital technologies and to address new and emerging risks, there will be an informal review every 12 months to ensure fitness for purpose.

**8.2.** This policy is monitored via two primary methods (as outlined in 5.5):

8.2.1.Concerns raised through security and web filtering alerting systems.

8.2.2.Concerns raised via issues raised with Service Desk (e.g. damaged equipment).

## 9. Equality Impact Assessment

*(Consider whether the policy or procedures may disproportionately impact any group.)*

| **Have you sought consultation on this policy?**<br><br>**Details:** | | ELT consultation has taken place. | | |
|---|---|---|---|---|
| **Could a particular group be affected (negatively or positively)?** | **Impact Y/N** | **Description of Impact** | **Evidence** | **Mitigation/ Justification** |
| Protected characteristics under the Equality Act 2010 | | | | |
| Age | Y | This policy is aimed to broaden the usage of IT both within and outside of College. As such, we would anticipate a positive impact upon younger persons as this ties in more closely with their usage of this technology (in general).<br><br>There is some potential for negative impact upon older persons, who are generally known to be lower technology users. This would be managed carefully when any new ways of working or services are brought in place. | | |
| Disability | Y | This policy should positively impact upon persons with a disability, by ensuring and encouraging respectful use of systems and communications, as well as supporting greater agility of use of systems (and the associated | | |

| | | | | |
|---|---|---|---|---|
| | | accessibility systems) outside of College, when physical attendance at College could be an issue at times for this group. | | |
| Gender Reassignment | N | | | |
| Marriage and Civil Partnership | N | | | |
| Pregnancy and maternity | N | | | |
| Race | Y | As per the disability group, the wider usage of accessible and agile technology, as well as translation technologies, should positively impact this group, as well as seeking to prevent inappropriate or discriminatory use of systems. | | |
| Religion or belief | Y | As above. | | |
| Sex | N | | | |
| Sexual Orientation | N | | | |
| Additional characteristics to consider | | | | |
| Young Persons in Care & Care Leavers | N | | | |
| Young Carers & Care Givers | Y | The additional flexibility sought to be embedded via this policy would positively benefit those young people who may have challenging personal commitments which could affect ability to attend College. | | |
| Young Parents | Y | As above. | | |
| Youth Offenders | N | | | |
| Those Receiving Free School Meals | N | | | |
| **If there is no impact, please explain:** | | | | |

**Appendix 1 – List of core IT systems and services**

The scope of this policy includes, but is not limited to, the following IT systems and services.

- All College owned IT devices, including desktop PCs and accessories (mice, keyboards, monitors etc), laptops, tablet devices, mobile phones, desk/fixed telephones, display screens, printers/copiers, and any specific technologies within curriculum areas (such as Virtual Reality headsets, voice assistants/speakers, etc).
- Email services
- Internet access services
- Wireless services
- File storage services
- HR systems
- Finance systems
- Learning Environment systems

- Student Records Systems
- Intranet/document management systems