South Devon College

IT Acceptable Use Policy

Policy No: P40

Document control

Version	Date	Author(s)	Notes on Revisions
1.0	June 2020	Paul Cooper	The previous combined *IT Security Policy and Internet Usage Policy* has been split into separate documents to enable expansion of Security Policy to meet Cyber Essentials and reflect the Digital Transformation Strategy
1.1	July 2021	Paul Cooper	Minor updates to reflect Cyber Essentials changes and remote working
1.2	Aug 2022	Ryan Cooper	Terminology updates and inclusion of managing web filter notifications
1.3	Sep 2023	Ryan Cooper	General update: Addition of staff & student communications, and new policies

Author	SLT Lead	Date of last PRG	Approval Committee	Approval Committee Date	Frequency of review	Next Review Date
Ryan Cooper	Kelly Sooben	15/9/23	SLT	3/10/23	1x year	Oct 24

1 PURPOSE

South Devon College ("The College") seeks to promote and facilitate the use of Information Technology for supporting the teaching, learning, research and business activities of the College; and may be used for any legal activity that further the aims and policies of the College. It is accepted that some limited and reasonable personal use will occur subject to it not interfering with the core functions of the College or those activities breaching this policy.

Whilst the traditions of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to the learners and staff of the College. This will help the College avoid accidental or malicious acts and associated financial, legal or reputational damage

It is the responsibility of all Users of the College's IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

This Acceptable Use Policy is intended to provide a framework governing the use of all IT resources across all sites on which the College operates. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

However this is just one aspect of a wider framework of e-safety, Safeguarding and Prevent strategies. For further information on this please refer to the Safeguarding Policy & Strategy, Positive Behaviour Policy & Strategy, Blending Learning, Content Capture, and other related policies.

2 SCOPE

This policy applies to all users including staff, students/pupils, visitors, contractors, partners, tenants and others, of the IT facilities provided by the College, are bound by the provisions of its policies in addition to this Acceptable Use Policy. It also addresses the use of the College's IT facilities accessed via resources not fully owned by the College, such as partner resources and the use of personal BYOD ('bring your own device') equipment.

It covers all user interactions using college provided logon ids, whether using personal or college equipment, and whether on college premises or elsewhere. These include participation in externally-hosted virtual events such as webinars, online collaborations and posting on any social media platform. (In addition, any user engaging in inappropriate behaviours using personal logon ids may be in breach of college policies and subject to sanctions.)

The IT facilities comprise all hardware, software, services, data and communication tools whether hosted on campus or provided by third parties including online Cloud and hosted services

3 ADDITIONAL POLICIES

Because the college uses the Joint Academic Network and its providers to access online resources this Acceptable Use Policy is taken to include the JANET Acceptable Use Policy, the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service.

Additionally, where the College provides access to the Eduroam service provided by Plymouth University, staff and students with this access must abide by Plymouth University's Acceptable Use Policy.

4 SUMMARY

Simply put, acceptable use covers six areas:

1. **IT Governance** – Don't break the law, do abide by the College IT regulations and policies, and do observe the regulations of any third parties whose facilities you access
2. **IT Identity** – Don't allow anyone else to use your IT credentials, don't disguise your online identity while representing the College and don't attempt to obtain or use anyone else's
3. **IT Infrastructure** – Don't put the College's IT facilities at risk by introducing malware, interfering with hardware, or loading unauthorised software
4. **IT Information** – Safeguard personal data, respect other people's information and don't abuse copyright material. Store data on secure college platforms such as OneDrive and SharePoint, don't use systems we are not licensed for such as Dropbox. Remember that mobile storage such as USB devices are not a secure way to handle information and must not be used to store personal or commercial information. If using BYOD to store College data, ensure the device is encrypted
5. **IT Security** - Ensure that any device you're using to access College systems, including Microsoft 365, have good security, are security patched and have anti-malware in place wherever possible
6. **IT Behaviour** – Don't waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world

5 DEFINITIONS OF UNACCEPTABLE USE

The College network is defined as all computing, communication, and networking facilities provided by the College. It covers all computing devices, either personal or College owned, connected to college systems and services whether on-premise, remotely hosted or Cloud-based.

The conduct of all users when using the College's IT facilities should always be in line with the College's values, including the use of online and social networking platforms.

5.1 Subject to exemptions defined in 6 below, the College network may not be used directly or indirectly by a user for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
- unsolicited "nuisance" emails or other messaging systems such as Teams
- material which is subsequently used to facilitate harassment, bullying and/or victimisation
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation

- material with the intent to defraud or which is likely to deceive a third party
- material which advocates or promotes any unlawful act
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party or
- material that brings the College into disrepute

5.2 The College Network must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:

- intentionally wasting staff effort or other College resources
- corrupting, altering, or destroying another User’s data without their consent
- disrupting the work of other users or the correct functioning of the College Network
- denying access to the College Network and its services to other users
- pursuance of commercial activities (even if in support of College business), subject to a range of exceptions

5.3 Any breach of industry good practice that is likely to damage the reputation of the JANET network will also be regarded as unacceptable use of the College Network.

5.4 Where the College Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College Network.

5.5 Users shall not:

- introduce data-interception, password-detecting or similar software or devices to the College’s Network
- seek to gain unauthorised access to restricted areas of the College’s Network
- access or try to access data where the user knows or ought to know that they should have no access
- connect to College infrastructure with any tabs, relating to any points in 5.1, already open within their browser on personal devices
- carry out any hacking activities
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software
- share their login details with anyone else whether a learner, member of staff or someone not directly associated with the college
- use another learner’s or staff member’s login details, or attempt to access anyone else’s account unless as part of an investigation or legitimate access request (see section 7.3)
- store any College data including emails and sensitive data on any system not licensed or sanctioned by the college, such as personal Dropbox accounts

- use College email accounts with @southdevon.ac.uk when setting up personal Internet accounts (for online activity or App stores) or as points of contact for personal purposes

6 EXEMPTIONS FROM UNACCEPTABLE USE

6.1 There are several legitimate academic activities that may be carried out using College information systems that could be considered unacceptable use. For example, research involving defamatory, discriminatory, or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques. In such circumstances advice must be sought through the College Leadership Team (CLT) and Senior Leadership Team (SLT). In each case documented approval/denial of the request will be recorded.

6.2 Any potential research involving obscene or indecent material must always be approved in advance with SLT and clear scope agreed, along with any records that need to be captured of specific accesses. If a member of the College community believes they may have encountered breaches of any of the above, they must report this immediately to their CLT Head who will liaise with SLT.

7 COMMUNICATION BETWEEN STAFF AND STUDENTS

7.1 Staff must ensure that, other than instances which are appropriate as part of their professional role, or which is considered a safeguarding matter:

- They establish safe and responsible online behaviours
- Communication between staff and students, by approved methods, should take place within clear and explicit professional boundaries
- They are circumspect in their communications with students to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming
- All communications are transparent and open to scrutiny in relation to Subject Access Requests
- They do not share any personal information with a student
- They must not request, respond to, or view, any personal information from a student
- Their personal social networking sites should be set to private
- They will never use or access the social networking pages of students
- They must not communicate with students from non-College accounts or personal phone numbers

More information around social media usage can be found in the Code of Conduct which can be found on the Policies and Procedures page of the Strategic and College Information Hub.

8 MONITORING

8.1 The College records and monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of:

- The effective and efficient planning and operation of the IT facilities
- Investigation, detection, and prevention of infringement of the law, this policy or other College policies
- Investigation of alleged misconduct by staff or students

8.2 The College will comply with lawful requests for information from government and law enforcement agencies.

8.3 Where there is a requirement to access the account, workspaces, email, and/or individual IT usage information of a learner or member of staff, documented authorisation must be obtained from the Head of IT Services or Vice Principal – People and Resources.

8.4 IT Services staff may monitor computers during active sessions, generally for assistance purposes but also where there is risk that a user is using a system in breach of applicable laws or college policies. Monitoring for assistance purposes will require permission from the end user.

8.5 All activity on computers being monitored is visible and any inappropriate activity may be recorded for disciplinary action. When requested by a member of SLT, IT Services staff may also carry out monitoring checks on staff computers and usage.

8.6 If the request for access is related to a staff disciplinary investigation, this will be managed wholly through the Head of People who will work with IT Services.

8.7 Automated notifications are in place to capture attempted access to blocked and restricted content detailed in Smoothwall’s full ruleset list (see appendix 1).

9 CONSEQUENCES OF BREACH

In the event of any failure to comply with the conditions of this Acceptable Use Policy by a User, the College may in its sole discretion:

9.1 Restrict or terminate a user’s right to use the College IT facilities.

9.2 Withdraw or remove any material uploaded by that User in contravention of this Policy.

9.3 Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

9.4 Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the College’s Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

STATUTORY FRAMEWORK/PRINCIPLES

The use of College IT systems and resources are subject a number of statutes and regulations including:

- the *Copyright, Designs and Patents Act 1988*
- *the Computer, Copyright Software Amendment Act 1985*
- the *Computer Misuse Act 1990*
- the *Data Protection Act 2018* (commonly referred to as GDPR)
- the *Electronic Communications Act 2000*
- the *Protection of Children Act 1978*
- the *Police and Criminal Evidence Act 1984*.The *Regulation of Investigatory Powers Act 2000*
- Trade Marks Act 1994
- Criminal Justice and Public Order Act 1994

Copies of these documents are available online at http://www.opsi.gov.uk/

10 MONITORING AND REVIEW OF POLICY

This policy will be monitored by IT Services and the Senior Leadership Team. This policy will be approved by the Vice Principal – People and Resources. Any changes to this policy or how the policy is enforced will need to be agreed before implementation. Failure to comply with the policy will be dealt with through the College's Disciplinary Procedures.

Actions	Date
Signed off – Ryan Cooper	September 2023
Signed off – SLT	03/10/2023
Next Review due	October 2024

11 RELATED POLICIES AND DOCUMENTATION

- IT Security Policy
- IT Staff Device Return Policy
- Data Protection Policy
- Child Protection/Safeguarding Children & Vulnerable Adults Policy
- Code of Conduct for Staff

12 APPENDICES

Appendix 1 – Smoothwall Safeguarding Notifications

A Safeguarding level is calculated for each breach, providing a visual indication of the severity of the breach:

- Danger — Red label, breaches with this level should be acted upon immediately
- Caution — Yellow label, you should take the necessary action with these breaches
- Advisory — Blue label, this level advises that a Safeguarding breach has been detected

Full Smoothwall Ruleset List: About the safeguarding full report (smoothwall.net)