South Devon College

IT Security Policy

Policy No: P41

Document control

Version	Date	Author(s)	Notes on Revisions
1.0	Feb 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	Jul 2021	Paul Cooper	Updates for Cyber Essentials, Multi Factor Authentication, default passwords and BYOD.

1 PURPOSE AND SCOPE

Electronic data and systems underpin every aspect of South Devon College ("SDC, "The College"). This policy ensures that this data, and access to it, is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of information.

This Policy applies to all users of College IT related information systems and sets out College policy regarding the accessing of information, giving guidance in accordance with current legislation and best practice initiatives.

In general, the 'Principal of Least Privilege' will drive the policy where possible and practical. Simply put, this allows a user or system the minimum access to IT components and data that it requires to perform its function, reducing the risk of system compromise and reducing the areas that need to be assessed if a system does become compromised.

This policy is designed to exceed the requirements of Cyber Essentials, and incorporate best practices including those from the National Cyber Security Centre (NCSC) and ITIL v3

The Policy objectives are to ensure that:

a. the integrity and security of all electronic systems is maintained;

b. all information is stored in a secure manner and that appropriate safeguards are in place to prevent improper access;

c. any attempts to gain improper access to information are detected and recorded accordingly;

d. College information systems are not compromised or used for unauthorised activities;

e. only authorised members of staff can collect and view pertinent information, which must then only be used for legitimate purposes;

f. information is only relayed to other legitimate and authorised users both inside and outside the College.

2 DUTIES OF THE COLLEGE

It is the responsibility of the College to implement and enforce the aspects outlined in this policy, and compliance with this Policy and any associated procedures is compulsory for all staff and learners. Anyone

who fails to comply with the Policy may be subjected to disciplinary action under the College disciplinary policy.

3 DEFINITIONS

Throughout this policy, 'the College' refers to all College sites, and also covers use of (or access to) IT equipment, systems and services from any non-College site.

Trusted device: a piece of IT equipment managed by IT Services or its agents which is centrally managed and elevated access is restricted to reduce the risk of compromise through malware.

Untrusted device: A piece of IT equipment where elevated access is available to end users, which increases the risk of inadvertent compromise through typical malware propagation, and where security updating is not enforced through automated College mechanisms. This includes BYOD, whether purchased by the end user or provided by the College.

Core Network: The central 'internal' area of the College's network which is protected by firewalls and access controls, and where the central on-premise data is stored. All equipment on this network will be under direct control of IT Services or its agents and is considered 'trusted devices'.

Perimeter Network: The edge of the College network which connects to the Internet. All physical connections between the College's internal network and the Internet will be protected by a firewall.

Continual Service Improvement ("CSI"): an ITIL practise based on the Plan-Do-Check- Act (PDCA) closed loop feedback mechanism to review outcomes in order to improve service.

4 PHYSICAL SECURITY

Infrastructure devices including servers and network switches are located in secure rooms or locked cabinets, with access restricted to specific staff. Where possible this will be via keycard access, to allow greater granularity of access and all accesses to be logged.

All fixed and mobile endpoint IT devices excluding phones (e.g. desktop computers, display screens, laptops and tablets) owned by South Devon College are labelled using a secure ID tag. They are also security marked with a 'Smartwater' chemical fingerprint, ensuring they can be traced in the event of theft.

All IT equipment is recorded in a central inventory, with owners allocated to all mobile devices to ensure accountability in the event of recall (e.g. for upgrades) and to ensure that equipment is managed through ownership changes e.g. staff leaving or equipment redeployment.

5 LOGICAL SECURITY

5.1 Physical network ports

All physical network ports will be configured to prevent unauthorised access from untrusted devices which may be deliberately or accidentally carrying malware.

5.2 Wireless Networks

Access to the wireless networked will be determined by a combination of device type (trusted or untrusted) and user type. This will ensure that the core network is protected from untrusted devices, and will ensure that a level of access is available to all users, including ad-hoc visitors. This differentiation of access will also allow the College to prioritise resources where there is a risk of contention, to ensure that core College activities take precedence over casual or personal use.

5.3 Network Segregation

The College networks are split into a number of sub networks ("VLANs") in such a way to reduce the risk of a compromise in one area affecting another. Access between VLANs is only provided where the access is specifically required, and even in that situation access will be provided at the lowest granularity possible, for example to allow a system monitoring tool to view a building management system but not other building system nodes on that sub network.

5.4 Single Sign-on

A user account will require access to all appropriate resources across a number of on-premise and cloud-hosted systems and data repositories. Where possible, this will be achieved using single sign-on i.e. the user's account will work across these disparate systems. This simplifies security and the need for managing multiple user ids and passwords. In situations where single sign-on is not available, or the facility to achieve this is not cost-effective, separate accounts may be needed. One example of this is Symmetry finance system, where user logins are managed separately by the Finance team with a different naming convention and password policy to the rest of the network.

5.5 Device Software Firewalls

Where a device has its own firewall facility e.g. Windows Servers and Workstations, these must be enabled and initial configuration using a 'deny all' rule and adding exceptions as needed. This provides an additional layer of protection against compromise, especially if a system inside the College network is infected with malware and attempts to infiltrate other College systems. These firewalls must be configured so that they cannot be modified by Standard Users to prevent accidental or deliberate misconfiguration.

6 FIREWALLS

Any logical connection from the College network to the Internet must be routed via a firewall which will provide protection and, where possible, automated monitoring to alert when the College network is being probed or attacked. This does not include physical broadband or private circuits connecting one College campus to another as that traffic will be protected via an encrypted virtual private network or similar and logically is a part of the seem to be part of the College network. All accesses will be restricted as much as possible to specific devices, ports and traffic type (UDP/TCP etc) and any alterations to the firewall allow/deny lists must go through the Change Management process and require a business case to describe risk/impact.

7 NETWORK TRAFFIC ENCRYPTION

To reduce the risk of interception, data must always be encrypted to a suitable standard where technology permits. Inside the College's private campus networks this will be achieved using Transport Layer Security ("TLS"). The TLS version used must be currently supported, and will need to be assessed to ensure that updates are applied to counter any identified weaknesses.

If the data is travelling between College sites across external bearer networks e.g. dedicated BT circuits or Broadband, the data must be encrypted using IPsec e.g. using a Virtual Private Network ("VPN") product. Current standards and best practices will be defined by the NCSC's Cloud Security Guidance.

8 WEBSITE TRAFFIC

All data presented by College systems to web browsers, including dashboards, traditional websites and SharePoint, must use HTTPS. This applies whether the server and clients are internal to the College's network, external or a mix of both.

9 PROXY SERVERS

Most access to external data is provided via a web browser which will be on a machine in the College network. This provides a significant risk as many websites are deliberately or inadvertently configured or hijacked to disseminate malware. In addition, the College has a duty of care to its staff and learners to protect them from inappropriate or illegal content. In order to mitigate these risks, all web traffic will be relayed via a proxy server which will be configured to allow or deny traffic based on a set of rules contained in a profile. Each group of users (for example High School students, HE students and staff) will be allocated a profile balancing their needs against the College's duty of care.

The only general exception to this is HE students and staff who make use of the Eduroam wireless network. Traffic on this network is not managed by the College, instead it is transmitted to Plymouth University who then utilise their own proxy service and profile.

The College Proxy Server will be configured to manage its access lists and rules via an automated subscription to a suitable provider. This ensures its blacklist and rules sets are kept up to date.

Exceptions to the standard rules, generally to whitelist a section of an external site, will be managed via the Change Control process and will not be granted unless the risk has been evaluated and appropriate approval is obtained.

All browser traffic is also tracked and recorded against users' network accounts, and can be used for investigation or reporting if required.

10 USER ACCOUNTS

10.1 Standard Users

All Staff are entitled to a network and email account for the duration of their employment by South Devon College, as authorised by Human Resources or the Assistant Principal. Line managers will authorise additional access to the College systems required for the performance of their duties.

When a learner is enrolled in the Student Records System, an individual network and email account is created for the duration of their studies at South Devon College. Access rights may be restricted or withdrawn during disciplinary action.

Access to the computers and systems at South Devon College is restricted to authorised persons only through use of of a unique network account created specifically for that person.

There is limited use of shared accounts by exception, these typically provide kiosk-style access and will not give access to personal information. Where shared accounts are used, a staff member must take ownership of the account and be responsible for all activities carried out under its login id, password changes etc.

a. Exam Accounts - controlled by exams dept to allow students to log onto an exam PC. These are single accounts used by one user on one pc at a time.

b. Teams Accounts - Controlled by dept admins to log onto a 'front of class' PC in order to run a remote lesson. Separate account used for each classroom.

c. Display Screen accounts - used by digital screens so lecturers can cast their own device to the display screen. Accounts don't have any privileges.

d. Controlled Assessments - Created ad-hoc and assigned to individual students in order to complete assessment work.

e. Department shared accounts - Issued and controlled by some departments to allow students to log onto a PC before enrolment has fully taken place. These are used for single students at a time and only in classes with open adverts so pre-enrolment is not possible.

f. Where these accounts are used as a temporary 'pool' e.g. for accessing online exams, the password must be reset and the account profile reset between uses. At no time must the same account be used simultaneously by multiple people.

The College requires all users to adhere to the following guidelines:

a. users will not attempt to gain unauthorised access to College IT systems;

b. passwords must be a minimum of eight characters in length, including at least one capital letter and one number, and must be changed at least every two years or when it is suspected a compromise may have been attempted

c. any temporary passwords issued must be changed at first use;

d. passwords must never be written down or disclosed to another individual or organisation;

e. passwords must never be sent in the form of clear text e-mail messages.

Multi-factor authentication (MFA) will be required for staff login outside college campuses on each device used by the member of staff, including personal owned devices. User verification will need to be refreshed in the following scenarios where the user:

1. has signed out of 365 and back in on the device

2. is signing on from a different device or browser
3. has had 14 days of inactivity on the device
4. It has been over 90 days since you last used MFA to sign in
5. Your session has been revoked by a system administrator

Users are responsible for the secrecy and integrity of their passwords. The College will consider password sharing a breach of this Policy (subject to shared accounts above) and this may result in disciplinary action being taken by the College.

User accounts will be disabled when staff and learners have left the College to prevent unauthorised access. Exceptions may be required in order to keep specific email accounts open for important College business to be accessed by remaining staff members; this will need to be requested by the relevant Section Head (or higher) together with an end date. In this situation email forwarding will be set up to another SDC email address or, where access to a leaver's storage is required for a period of time, access will be given to nominated user(s) by the relevant section head.

In the event of the suspension or investigation into conduct of a member of staff or learner, individual accounts may be accessed by authorised members of IT Services to assist with the investigation. Requests for access will come via a member of SLT, using the Information Access Request form (see Appendix 1).

10.2 Elevated Access

Application owners, and IT Services staff, will require elevated access in order to carry out system monitoring, maintenance and application work. In all cases this must be achieved using a separate login from the standard user account which they will continue to use for general line-of-business activities.

Granting and revoking access will be managed via the College's Change Management process to ensure a clear audit trail of request and approval, and the specific access given will be based on the user's role. This prevents privileged accounts from having access to features that are not required for their role, minimising access to personal data and reducing the risk of accidental or deliberate harm or access to systems.

In some situations, where the highest level of privilege is required, an additional account is provided solely for that purpose. Examples of this include the Linux Root user, the Active Directory Enterprise Admin and Schema Admin roles, and the database sa user.

Server and domain-level elevated access accounts will not have access to the open Internet, this prevents any browser-delivered attack from utilising the elevated account privileges to cause damage. Accounts which have elevated access to domain-based desktops only will have internet access as this is needed in many cases for software installation to complete successfully. Anything which needs to be downloaded and installed must be copied down using a normal or desktop-admin account, and the software scanned for malware prior to testing and subsequent implementation.

The password policy for accounts with elevated access is the same as for standard users, although MFA will be required on every use to further reduce the risk of compromise.

Elevated accounts will be reviewed at least annually to ensure they reflect the requirements of the organisation.

10.3 System Accounts

These are accounts that are used by services or processes to access other systems or data and often require elevated access. Typical examples would be system monitoring (requiring administrator level access to systems it monitored) and data collation (requiring access to personal data from a number of sources). Each system account must have a clear description, and be recorded in the CMDB with a justification, owner, and detail around what it accesses and why. This will typically be included within a system's documentation.

The password requirements for these are for a complex, non-dictionary password using one or more upper and lower case letters, numbers, and special characters. Password length must be in excess of 20 characters. If one or more of the systems the system accounts accesses cannot accommodate this password structure a weaker password may be used but this needs to be fully risk assessed and approval obtained through the Digital Strategy Group using the Change Control mechanism.

In no circumstances are these accounts to be used by staff other than for troubleshooting technical issues affecting the associated service.

System accounts must be reviewed at least annually to ensure they are still required, their access is appropriate and minimal, and password reviewed and changed where risk is identified. Access should also be reviewed as part of the upgrade process for the system.

10.4 Accounts on third-party systems

Staff and learners are encouraged to sign up to forums and knowledge bases that will enhance their learning, and in these situations it is reasonable for them to sign up using their College email address. However, they must use different passwords from their College login to protect their College access in the event that one of these services are compromised and their login details and password are obtained by a third party. (The use of a password manager is strongly recommended to facilitate this.)

Where the external service is used by the College and contains confidential or sensitive data, for example IT vendor portals containing licensing information or access to user information such as account names, the password requirements are for a complex, non-dictionary password using one or more upper and lower case letters, numbers, and special characters with a length of at least 20 characters. Again, it is recommended that a suitable password manager is used to store these.

10.5 Use of College accounts for personal purposes

College email addresses must not be used to sign up on a third party system for personal purposes e.g. personal shopping. Access to personal email domains such as yahoo and outlook.com is allowed and personal email addresses should be used for signing up to such services.

10.6 Password Managers

Where users connect to multiple external systems, it is important not to use the same login details and password. This removes the risk of a set of credentials stolen from one site providing access to multiple sites, some of which could be used for financial or College reputational purposes.

IT Services will recommend a suitable password manage on request. The encryption method of the password database and how the application behaves when active (e.g. not storing any sensitive data in plain text in the computer memory) alongside its history and reputation will be assessed to ensure the product recommended is highly secure.

11 ACCESS TO RESOURCES BY SDC STAFF AND LEARNERS

The College will ensure that the default behaviour of IT systems will be to hide all files and data from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user.

This access will be managed via Active Directory (“AD”) group membership where possible, where each filestore area or data set will be assigned a data owner (e.g. the Finance Director will be responsible for all Finance filestore and database access). The group will be populated with users who require access, and the data owner will be required to approve or reject requests to modify the membership of that group and so change who has access to the data.

Where AD groups are not available, a similar mechanism will be used, and a data owner will need to be identified and recorded to review requests to modify the access list. In no circumstances are individual users to be granted direct access to file or data resources except for personal OneDrive file sharing.

11.1 Staff Changing Roles

Where a member of staff moves from one role into another, any system access must be reset to ensure it reflects the requirements of the new role and does not introduce ‘permission creep’ where a user, over a period of time, acquires access to systems and data that are not required for their role.

It is recognised that there may be a business case for retaining access to systems and data for both roles for a period of time to ensure handover/smooth transition to reduce the impact on the college. In this case the request must be approved off by section heads covering both roles as well as the College’s Data Controller, and must have a fixed duration no greater than three months at which point access will be reset to the requirements of the newer role.

12 ACTIVITY MONITORING

All systems, programs and data are the sole property of South Devon College and their use is subject to monitoring. South Devon College monitors and logs activities, including:

- Internet traffic
- Network connections
- Network access and attempted access
- Software programs accessed
- Printing statistics
- Microsoft 365 access and activity

It is also possible for IT Services to monitor learner computers during active sessions. 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.

12.1 Data Backup

The primary reason for backing up data is to keep copies in case of a disaster, for example a software failure that destroys data, hardware failure of a computer making data inaccessible, or environmental damage to computers such as fire.

12.1.1 On-Premise

Backups of the data on central servers are created in case of a disaster affecting the servers or the databases held on them. They are not intended for recovering individual files or emails belonging to particular users. The backups are structured in the most efficient way for recovering complete systems or databases. Where requested, IT Services staff may be able to recover individual files, emails or other items of data.

Backups are created each night using automated systems. Therefore any data created and deleted on the same day will be irretrievably lost.

12.1.2 Cloud-based

Services such as Microsoft 365 provide a much more granular recovery process for individual files, along with version control which allows users to roll back changes to a file, or create a copy from a previous version e.g. to compare changes. This functionality will be a requirement of any future cloud platform.

13 HARDWARE

All requests for hardware including network devices, servers, storage platforms, printers and endpoint devices will be security assessed to ensure it meets the requirements of the College (essentially whether it fully supports the requirements of this policy), can be centrally managed and updated at the firmware level. The process for monitoring the firmware, reviewing vendor updates and assessing risks and mitigating against them by patching will be key to authorising the equipment to be used for College purposes.

Low-level access to the hardware (for example the BIOS configuration menu on a pc) will be protected by a strong password in line with section 10.3 System Accounts.Elevated Access

14 SOFTWARE

14.1 Operating Systems

Servers and endpoints which are deployed by IT Services will use an operating system with a configuration and feature set selected to maximise security and ensure manageability. In most cases this will be a Windows platform which will then be incorporated into the College's Active Directory and will be managed through Microsoft Endpoint Manager. Non-Windows operating systems will be by exception only (for example Linux) and will require careful specification to ensure that it will have the same level of manageability and security.

14.2 System Applications

At the core of data collection, collation and presentation is the software that powers the College's IT networks and systems. This comprises operating systems and applications including any higher level plugins such as ActiveX controls etc.

Requests for systems and applications will be made from different areas across the College and in all cases IT Services will be engaged to work with the requestor to prepare a Change Request proposal which will be used to risk assess, cost and ascertain suitability for use within the College. In all cases, the ability and track record of the vendor to produce and make available security patches will be a prime consideration. Additionally, any Internet access and consequent firewall changes required by the software will need to be risk assessed as part of the overall decision process on whether to proceed with utilising the software. The change will be reviewed at an appropriate level based on the risk, for example anything which requires external firewall changes will need to be reviewed by the full CAB and approval will need to be at SLT level.

If approved, all configuration, work flow, data access and infrastructure configuration changes needed to support the software must be documented prior to going live.

14.3 Data Flows

Any data flows into and out of an application will need to be accurately documented to ensure there clear understanding of what data is being moved across systems, and any modifications that are made to this data by either the receiving or transmitting systems. All data flows will need to be secure and encrypted to an agreed industry standard such as TLS 1.2 regardless of the category of the data it is moving (it will be assumed that any data is sensitive or personal).

14.4 Endpoint Apps

All endpoint apps must be compliant with the same requirements as system applications. They must also come from legitimate sources i.e. Google Play Store for Android and the App Store for Apple.

In addition, any local data storage must be assessed and assurance given that it is not held in unsecured files before the application can be approved for use.

14.5 Patch Management

All software, whether operating system or application, must be supported by the vendor, who will provide patches to mitigate vulnerabilities that are discovered. IT Services will, as part of the initial commissioning of the software, initiate a process to ensure that these patches are flagged to the College. IT Services will then assess the patch and schedule deployment. Deployment will be within 14 days for patches which resolve a vulnerability classified by the vendor as 'critical' or 'high risk' and within 28 days for all other classifications.

14.6 Security Patch End of Support

During the lifecycle of the software, if security patch remediation is no longer provided by the vendor, for example a newer version replaces the version the College purchased, the software must immediately be removed from all College devices.

14.7 Licensing

All software in use on College equipment must be legally sourced and licensed. Where different licensing options or models are available, IT Services will work with relevant Sections to ensure that the correct option is selected and will educate staff where necessary to ensure that they do not inadvertently breach licensing and risk bringing the College into disrepute or legal and financial risk.

14.8 Review

All software will be reviewed at least annually to ensure it is still required, fit for purpose, and at the correct licensing level.

14.9 Removal

When software is no longer required, or when its licence has expired, it must be removed from the systems it was installed on. It is not sufficient to disable components as this may leave an exposed attack vector on the host system or inadvertently allow unlicensed or vulnerable software to become active.

If software that needs to be removed required any firewall rules (either on local devices or at the network perimeter), these rules must be reversed to ensure the firewall remains as restrictive as possible.

14.10 Restrictions

The installation of new software is barred to all users, on any College computers. This prevents breaches of security or damage to the network from installers which may come from untrusted sources and contain malware, Trojans, or other potentially harmful electronic file, and helps to ensure software licensing remains compliant with vendors' terms. Only authorised staff are permitted to install programs onto computers and only after licence compliance has been verified by IT Services.

15 CLOUD SERVICES

The Digital Transformation Strategy states that the College has adopted a 'Cloud first' approach to providing access to data, and over time this will reduce the number of on-premise systems. This will also increase the amount of College data (including personally identifiable information) that is held on systems and networks not directly under the control of the College's IT Services team.

Where a service is required which will involve storing College data on such systems and networks, rigorous evaluation will take place to ensure the potential providers are suitable. This will include their overall security accreditation (ISO 270001, PCI DSS, SOC2 etc), a review of any known breaches in their history and subsequent lessons learned, alongside ensuring that any data belonging to the College is stored in an acceptable geographic location. Any contracts subsequently entered into will provide for regular reviews to ensure their security accreditation remains valid, and in any case their accreditation must equal or be superior to that of the College.

15.1 Microsoft 365

The College has chosen the Microsoft 365 platform and application suite as the strategic platform for cloud-based document and data storage alongside collaboration using SharePoint and Teams. The College will monitor overall system status and ensure that it follows best practices to maximise the security of its data with the 365 ecosystem.

Guidance has been issued to staff to assist in transforming from the on-premise mapped drive model to a use of OneDrive, SharePoint Hubs and SharePoint Bases.

Sharing OneDrive documents should be very limited; this is personal storage and should not be used for holding documents that are for a section to use – these should be stored in a Hub or Base.

In all cases, generated links will be limited duration and will default to specific people. This removes the risk of files or folders remaining available, especially to external parties, where content changes may expose confidential or sensitive data.

15.2 Google

Although the College has a Google presence, this is no longer supported and staff are encouraged to move any data and/or documents across to 365. IT Services will only provide best-efforts support to staff and learners reporting issues within this ecosystem.

16 SECURE TRANSFER OF DATA AND ACCESS OUT OF COLLEGE

The College recognises that personal data may be accessed by its staff when out of College, or transferred to other stakeholders or external agencies. In these circumstances:

- Users must take particular care that computers or removable devices which contain College based data must not be accessed by other users (e.g. family members) when out of College.

- When sensitive or personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should use secure remote access to the management information system, learning platform, or data area.
- The recommended method of accessing College data and systems remotely (and securely) is to use the College Remote VDI Service or Microsoft 365.
- College staff must be vigilant when transferring data to an external organisation or individual, to ensure there is no risk of the data being accessed by a third party who does not have rights to access the data.
- Data is not to be taken or transferred outside the UK and Northern Ireland, and advice must be taken from the Assistant Principal responsible for Systems and Information if this is required.
- Users must not use unapproved third-party providers for storing or transferring College data (such as personal email, personal Dropbox accounts etc). These are outside the control of the College and data security in such services cannot be guaranteed, neither can the data be removed by the college in the event the user leaves the College.
- Email traffic between systems is encrypted, but the email contents are open at the receiving end. In order to provide additional security for especially sensitive data, the email should be encrypted at the sender's discretion by using the Encrypt option in Outlook.

16.1 Portable and Home Devices

This covers laptops, tablets and phones used for College business, whether supplied and configured by the College, BYOD or home devices.

Personal devices are permitted on campus, but are the sole responsibility of the individual owner. Technical advice can be provided by the IT Helpdesk where issues arise, however the College is not responsible for personal IT equipment or devices and support will be on a 'best endeavours' basis.

All College provided devices must be configured for full local storage encryption, compliant with FIPS140-2.

In general, personal devices must not hold local copies of files or data that is sensitive, personal or confidential. Instead staff must make use of the College's Microsoft 365 services to access and work on the files or data, saving them directly back to the Cloud. Staff must be especially vigilant with Internet downloads, and frequently check the local Downloads folder on their device and remove anything that may contain personal or business-sensitive data associated with the College.

16.1.1 Personal Device Security

Where functionality is available, staff must ensure that their devices have a good level of security. This includes:

a. Ensuring all operating system and applications are kept up-to-date with security patches, and critical updates are installed within 14 days of release. Ideally all application and operating system updates will be set to automatically update.

b. Enabling and maintaining the device's software firewall

c. Removing applications that no longer have security patches provided by the vendor

d. Installing adequate malware protection and ensuring it is allowed to update automatically

e. Not installing any applications from untrusted sources

f. Not rooting/jailbreaking Android/Apple devices or installing apps from non-official portals.

g. Disabling auto-run for any removable media devices.

Although some of these may be seen as intrusive, they will provide a good level of security for personal use and reduce the risk of personal data loss through security compromise/ransomware etc.

16.2 Removable Media

Portable media covers read/write devices such as USB memory sticks and portable hard drives. These must not be used to hold any sensitive, personal or confidential files or data relating to the College, its staff or learners. Again, the College's Microsoft 365 services must be used to access data where traditionally a USB stick would have been used.

16.3 Removable Media Exception

If a member of staff is for example presenting at a conference or seminar, it is permissible to use removable media to hold a copy of the electronic resources, presentations etc but only where these resources do not contain sensitive, personal or confidential information.

17 EMAIL

17.1 Filtering and monitoring

Alongside web browsing, email is a common method for attackers to attempt to compromise an organisation's systems and data. The College will utilise a filtering technology to assess all email coming into the College or exiting the College externally to detect common threats such as malware and phishing attempts and prevent their onward transmission into the user's mailbox. This filtering technology will also use a quarantine mechanism to pause emails which although not clearly flagged as carrying damaging material are suspicious. These will be reviewed on a case-by-cases basis and passed to the intended user where no threat is discovered.

17.2 Automatic Forwarding

This is considered a security risk and best practice recommends blocking this capability. This reduces a number of risks including:

- Compromised accounts often create an auto-forward rule to continue to extract data from the college once the initial breach is resolved.
- Forwarding to external providers may affect compliance issues since the messages are no longer under the control of the college and may not be available for safeguarding issues or legal hold.
- Email addresses are considered personal information, so any forwarded emails which go to more than once user may be breaching GDPR.

Due to these risks, automatic forwarding of staff and governor email from the southdevon.ac.uk domain will be blocked.

18 REMOTE ACCESS BY SDC STAFF AND LEARNERS

External access to on-premise College IT systems within the core network is only available to users with a valid login and password and will be provided via a remote desktop session. The remote desktop will be presented as a 'pane of glass' i.e. there is no facility to transfer files into or out of the remote desktop to the device the user is connecting with. This removes the risk of core system compromise.

Any authorised user logging in to the College network from home or from another external access point must comply with the following guidelines:

- Viewing of College data and documents must not be shared. At home this would be family members etc, if remote access is used in a public place extreme care must be taken to ensure the display cannot be overlooked.
- The remote session must be logged out when the user has completed their tasks to free up capacity.

19 INFORMATION ACCESS BY THIRD PARTY ORGANISATIONS

Access to College IT facilities by third parties will not be provided until conformation of agreement to the College's Acceptable Use Policy has been provided, and the third party has demonstrated compliance to a security industry standard equal or superior to that achieved by the College. The College will also utilise data sharing agreements in all situations when the information being disclosed can be classified as personal or confidential data.

This access will only be granted when required, and will be disabled at all other times. Access requests will be managed via the College's Change Control system.

20 DISPOSAL OF DATA

The College will comply with the requirements for the safe destruction of personal data when it is no longer required.

Rather than seek to apply different standards for data disposal based on its categorisation, the College will assume that all data requires treating as if it was personal. To achieve this and assure effective sanitisation of media devices holding such data, any destruction must meet HMG Infosec Standard 5, NIST 800-88 or equivalent.

21 VERIFICATION

At least annually, the College will engage with a suitable security vendor to test a selection of elements to ensure that security practices remain compliant with this policy. Any omissions or exceptions will be reported and investigated as part of the IT Services CSI cycle.

22 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 Assistant Principal responsible for systems and information . 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 – Paul Cooper	05-Jul-21
Signed off – SLT	14-Jul-21
Next Review due	July 2022

23 RELATED POLICIES AND DOCUMENTATION

- Acceptable Use Policy
- Data Protection Policy
- Staff Code of Conduct

24 APPENDICES

24.1 Appendix 1: Staff Information Access Request form

<table>
<tr><td colspan="2">Staff Data Access Request form
This form should be copied into and email sent to the IT Service Desk who will then organise approval and subsequent access, ensuring a clear audit trail.</td></tr>
<tr><td colspan="2">This form is to request access to staff IT accounts for retrieval of data during absence, or the purposes of investigation. Access can be granted to staff emails, staff N Drives (My Documents) or OneDrive space, Internet usage/browsing history, or access to secure folders on the College Network.</td></tr>
<tr><td colspan="2">SLT member:</td></tr>
<tr><td colspan="2">Information required (including name/s of staff):</td></tr>
<tr><td>Date required:</td><td>Duration:
(typically one month, extended on request)</td></tr>
<tr><td colspan="2">Signed:</td></tr>
<tr><td colspan="2">Date:</td></tr>
<tr><td colspan="2">When completed, please give this form to the Head of IT Services, or the Vice Principal People and Resources</td></tr>
</table>