Reference Number: *P32*

ACCEPTABLE USE OF IT POLICY

Policy Review					
Author/Owner	**Position**	**Approved by:**	**Approval Date**	**Review Cycle Review Date**	**Published on Website Y/N**
Gareth Bevan	IT Services Manager	SLT Mark Bolton	22.10.26	Annually	Y

Document Control – Revision History (Policies only)					
Author/Owner	**Summary of Changes**	**Date**	**Version / Revision**	**Date last reviewed by SED**	**Recommend to SED Y/N**
Craig Cullen/ Michelle Dennett	Minor amendments to clarify points.	13.09.17		09.09.15	No
Craig Cullen/ Michelle Dennett	Minor amendments to KCSIE 2018	23.08.18		09.09.15	No
Craig Cullen	Complete rewrite of policy completed due to new technologies and systems implemented in 2019-20 to cover students and staff. Separate rewrite by Michelle Joy for Student Handbook.	08.02.22	v1		
Gareth Bevan	Amendments due to OU review. Cyber Essential risks added.	21/06/23	v1.1		
Sian Deasy & Craig Cullen	Embedded formatting to ensure clickable links and heading formatting was correct. Amendments to font size, line spacing and alignment in line with Accessibility best practice guidance. Inclusion of summary document for students. Clearer references to where misuse of IT may intersect with disciplinary action for students and conduct expectations in 3.9.		v1.1		
Gareth Bevan	eSafety section added in relation to Filtering and Monitoring standards and KCSIE. BYOD expanded in relation to charging of devices. Updates to linked policies and procedures, general formatting and correction of job titles. Amendment to password policy.	22/10/24	v1.2		
Gareth Bevan	Clarifications to section 3.20.11 - Clarification on the connection to secure and unsecured Wi-Fi systems, from college devices. Amendments to remote access to college systems. 3.22	21/11/25	V1.3		
Gareth Bevan	Minor amendments to staff creation 3.2.1, other minor edits and formatting.	16/10/26	V1.4		

Initial Equality Impact Screening

Has anyone else been consulted on this policy and/or procedure? Craig Cullen

What evidence has been used for this impact screening (e.g. related policies, publications)?

Declaration (please tick one statement and indicate any negative impacts)

☒ I am satisfied that an initial screening has been carried out on this Policy and/or Procedure and a full Equality Impact Assessment is not required. There are no specific negative impacts on any of the Protected Characteristics groups.

☐ I recommend that an Equality Impact Assessment is required by the Equality and Diversity group, as possible negative impacts have been identified for one or more of the Protected Characteristics groups as follows:

- ☐ Age
- ☐ Disability
- ☐ Gender Reassignment
- ☐ Race
- ☐ Religion or belief
- ☐ Sex
- ☐ Sexual orientation
- ☐ Marriage & civil partnership
- ☐ Pregnancy & maternity

Completed by:	Gareth Bevan		**Position:**	IT Services Manager	**Date:**	21/11/25

Reviewed by Equality & Diversity Group: ~~YES~~/NO If Yes: Date:
I confirm that any recommended amendments have been made

Summary of Comments including Recommendations from Equality & Diversity Group Review:

Amended by Author:		**Position:**		**Date:**	

CONTENTS

1. PURPOSE OF THIS POLICY 4
2. SCOPE 4
3. POLICY STATEMENT 4
4. RESPONSIBILITIES 24
5. RELATED LEGISLATION AND DOCUMENTS 24
6. DEFINITIONS 25
APPENDIX A - Student Guidance: Using IT Appropriately at Yeovil College 27
APPENDIX B - Account Creation / Update / Deletion Process 29
APPENDIX C - Complex Password Rules 30

1. PURPOSE OF THIS POLICY

1.1. Yeovil College offers a wide range of IT Resources, encouraging staff and learners' digital skills; supporting and developing independent and collaborative learning skills.

1.2. To use Yeovil Colleges IT Resources, Users must agree to the responsibilities and conditions outlined in this IT Acceptable Use Policy.

1.3. If you do not agree or understand any aspect of this policy you must log out, disconnect, or stop using the IT Resource immediately. If you need any guidance on this, please contact IT Services (01935 845321) / helpdesk@yeovil.ac.uk.

1.4. Students can refer to Appendix A 'Using IT Appropriately at Yeovil College' for a one-page overview of the key principles of this Policy. This overview is designed to help students understand the core principles of Acceptable Use of IT, to subsequently aid in their understanding of this Policy. Appendix A is designed to assist understanding, not as a substitute for students taking the time to read through this Policy and understand its detail.

2. SCOPE

2.1. This policy applies to any activity undertaken both on college premises and off college premises, linked to Keeping Children Safe in Education - 3 September 2018. This includes anyone who uses any of Yeovil Colleges IT resources or services (including online services).

3. POLICY STATEMENT

3.1 User Accounts & Access Control

3.1.1. Access to Yeovil Colleges IT Resources is available via a User Account associated with an individual user.

3.1.2. Attempting to create, circumvent or elevate permissions of Users Accounts by any other method will result in disciplinary or legal action (in line with the Learner Disciplinary Policy[1] for

[1] Available at https://www.yeovil.ac.uk/policies-reports/

students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff[2]).

3.1.3. Users must take all necessary precautions to prevent unauthorised access to their user and system accounts. This includes ensuring they do not share, loan, write down, email, publish or communicate their User Account details.

3.1.4. Attempting to obtain another User Account's details by any method will result in disciplinary or legal action (in line with the Learner Disciplinary Policy for students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff).

3.1.5. Staff may be required to assist Learners with User Account details this must only be done with the Learners consent each time it is required.

3.2. User Account Creation

3.2.1. Staff Accounts

- Staff accounts will be provisioned via the Human Resources information system and automatically created using the information provided. IT Services will only create, change, or delete accounts, under the direction of the HR department.
- Appendix B shows the staff account creation process.

3.2.2. Learner Accounts

- Learners' User Accounts will be automatically created 1 hour after being enrolled on an active course. If any alternations are required to a learner's detail, Users must request this via the iZone Team.
- Learners' User Accounts will be automatically given an individual password, which will be shared with the learner's enrolment details.

3.3. User Account Removal

3.3.1. Staff Accounts

- Staff User Accounts will be automatically deactivated on the end date of their contract. This will be controlled via the HR department, reporting to IT Services. User account data (OneDrive & My Documents) will automatically be archived by IT

[2] Available to staff via 'Policies and Procedures' in the Yeovil College SharePoint.

Services for 12 months, before automatic deletion. Email archives will be kept for 36 months, before automatic deletion. User accounts that need to have extended access, before automatic deactivation, will be controlled by HR. This will be reported to IT services, with a clear deactivation date. User archive data access will be controlled by IT Services and access requests must be made via email to the IT Helpdesk, to show a clear audit trail.

3.3.2. Learners Accounts

- Learners' User Accounts can be disabled at any time by a staff member contacting the Learning Resource Centre or IT Services. A clear reason will need to be provided for the request and the tutor must be informed of this decision. All non-active Learners User Accounts will be automatically disabled on the completion of their course end date. Learner user account data will automatically be deleted 3 months after their course end date.

3.4. Guest Accounts

3.4.1. IT Services may provide Guest User accounts. This is under the discretion of IT Services, who will assess security concerns before the creation or use of an account. Guest accounts can only be requested by a member of staff via the IT helpdesk, to show a clear audit trail. These will only be available for set periods of time, mainly to support visitor, exams or contractor needs.

3.4.2. All guest user accounts with internet access must be associated with an individual, records of the use of these accounts will be maintained by the IT Services Department.

3.4.3. Guest WIFI is available for authorised visitors. Please refer to the BYOD section for more information.

3.5. Administration Accounts

3.5.1. Administration permissions to the domain and local computers are limited to members of the IT Services department only.

3.5.2. Special access and administration permission to systems and applications will only be granted with the system owner's permission.

3.5.3. Special access & administration group membership will be monitored and reviewed monthly, for audit and control purposes.

3.6. Access Control

3.6.1. Access to systems and resources are restricted by security permissions groups. To request additional access, please contact the IT Helpdesk for guidance or the system owners.

3.6.2. Access to IT Resources may be removed by system owners, the HR department or a member of the Senior Leadership Team by contacting the IT Helpdesk (helpdesk@yeovil.ac.uk).

3.6.3. All requests for permission changes must be requested by email to IT Services (helpdesk@yeovil.ac.uk) for a clear audit trail.

3.6.4. IT Services may monitor file access permissions. Any permissions deemed unnecessary or incorrect may be deleted at any time.

3.7 Passwords & Authentication

3.7.1 Yeovil College requires all User Accounts to have a complex password, details of the complex password requirements are detailed in Appendix C.

- Passwords must not be obvious or easy to guess.
- Passwords must be unique and must not be used for any other purpose or website.
- Passwords must be memorised and may not be saved unencrypted on electronic devices.
- Passwords may be changed at any time.
    - Staff should contact the IT Helpdesk for further assistance or advice on passwords.
    - Learners should contact the Learning Resource Centre or IT Services for further assistance or advice on passwords.
    - Alternatively, users can change their passwords in office.com, under their account settings.
- For the purpose of system security, IT Services may reset or otherwise disable access to an account at any time by approval of the IT Services Manager, Senior IT Services Engineer or HR.

- Passwords must remain strictly confidential, should never be written down or disclosed to anyone.
- Users are responsible for any activity which takes place while logged in using their User Accounts or college systems.
- IT User Accounts will automatically be locked out after 5 incorrect password attempts.
    - Staff accounts can be enabled again by contacting IT Services or on enabled Multi-Factor Authentication (MFA) services on Office.com. Three security questions may be asked against college data, to clarify user identity, prior to enabling the account.
    - Learner accounts can be enabled by the Learning Resource Centre, IT Services or enabled MFA services on Office.com. Three security questions may be asked against college data, to clarify user identity, prior to enabling the account.

3.7.1 The National Cyber Security Centre (NCSC) has published an article called "Three random words or #thinkrandom" which provides guidance on what makes a good password.

3.7.2 The NCSC Password Policy Infographic also explains how passwords are discovered & how system security policies can help.

3.8 Reduce Reliance on passwords

3.8.1 Yeovil College uses single sign-on (SSO) where available to reduce the number of passwords users are required to remember & enter. This is where systems read the account details of the PC you are logged into to, which then automatically log you in a system (if you have the rights associated permissions).

3.9 Multi Factor Authentication (MFA) or Two Factor Authentication (2FA)

3.9.1 Multi-Factor Authentication (MFA) will be used to improve the security of Yeovil College user accounts.

3.9.2 Users are required to provide a mobile phone number or download a mobile app to receive a Multi-Factor Authentication (MFA) code to access college systems.

3.9.3 Users will be asked to enter a code sent to their phone or authenticate on the App, when logging in from outside Yeovil College's network.

3.9.4 Users must use Multi Factor Authentication or Single Sign On services for any cloud-based logins that provide access to college resources or data.

3.9.5 College mobile phones will not be issued solely for MFA purposes. In some special cases, users that do not have access to a personal device can contact IT Services for loaned equipment to support this security requirement. This will be a hardware token that will generate a rolling unique MFA passcode.

3.10 Password Managers

3.10.1 A password manager is an App on a device or a web browser service that stores passwords securely, so users do not need to remember all their passwords. They can also create random, unique passwords for use when creating a new password or change an existing one. These are often a paid for resource or software that the college would recommend.

3.10.2 Yeovil College would recommend learners to use a password manager, to support safer password management.

3.10.3 Yeovil College supports staff within key departments, using a password management service. Staff are welcome to call the IT Helpdesk for advice on password management or request access to this service. Any associated costs will need to be agreed and budgeted for at department level.

3.11 Communication Systems

3.11.1 Yeovil College uses electronic communication methods to conduct official and legal College business. Communicating to staff and learners via electronic communication methods will speed the delivery of information and will offer sustainable and financial savings, by reducing mailing costs. All Users are given the appropriate account(s) to access these communications. Recipients will be expected to read all electronic communication relating to College business and when necessary, act as a result of communications received from the College. It is expected that staff and learners will monitor their College electronic accounts often, to receive the most up-to-date information from the College.

3.11.1 Full details are covered under the communications policy.

3.12 Data Security

3.12.1 To ensure data security, the College has a clear screen & desk policy.

3.12.2 This means:

- 3.12.2.1 Users must lock the PCs EVERY TIME they leave their computer or desk, even if it is only for a short period.
- 3.12.2.2 All printed documents with personal information must be kept in a locked draw or cabinet EVERY TIME Users leave their desk.
- 3.12.2.3 Passwords must never be shared. If someone else needs access to documents, emails, systems etc. Users must contact the IT Helpdesk for advice.
- 3.12.2.4 Users must not save any files or folders on College desktop screens. Users must save in the appropriate spaces i.e. OneDrive, Teams, Moodle and SharePoint systems. These resource spaces are backed up / version controlled to help protect college and user data. Yeovil College takes no responsibility for files or folders saved incorrectly on college desktop screens. Yeovil College has the right to delete any files and folders saved incorrectly, without notice.

3.12.3 Documents and data containing personal data must never be taken, copied, or downloaded onto personal computers or systems outside of the College's network. Refer to the P27 Data Protection Policy[3] for more details.

3.13 Monitoring and Logging

3.13.1 Yeovil College monitors and logs data for all IT Resources, including web services.

3.13.2 Monitoring and logging include:

- 3.13.2.2.1 Login / logout.
- 3.13.2.2.2 Location login / logout.
- 3.13.2.2.3 File activity.
- 3.13.2.2.4 Internet activity.
- 3.13.2.2.5 Communication.
- 3.13.2.2.6 Location tracking of equipment.

[3] Available at https://www.yeovil.ac.uk/policies-reports/

3.13.2.2.7 Screen capture or monitoring.

3.13.3 By logging into IT Resources, Users agree that data identifying users as an individual can be securely stored and used by Yeovil College to investigate breaches of this policy.

3.13.4 Where officially requested, data maybe be sent to local authorities for criminal investigations.

3.14 Safeguarding and Prevent

3.14.2 The following activity is actively monitored and logged as part of the College's responsibility towards multiagency safeguarding and PREVENT agendas:

3.14.3 The information which may lead to potential terrorism or extremist activity such as sites categorised as:

3.14.3.2 Intolerance
3.14.3.3 Personal Weapons
3.14.3.4 Terrorism
3.14.3.5 Violence

3.14.4 The information which may lead to a potential risk to young people or vulnerable adult's Internet activity including sites categorised as:

3.14.4.2 Adult entertainers
3.14.4.3 Adult sites
3.14.4.4 Child abuse
3.14.4.5 Pornography
3.14.4.6 Restricted to adults
3.14.4.7 Anonymous chat websites

3.14.5 Logs and information relating to Safeguarding or Prevent will be shared with the College's trained Safeguarding / Prevent team and may be shared with local authorities for further investigation.

3.15 **Online Safety**

3.15.1 The College has a responsibility to comply with the filtering and monitoring requirements as set out in Keeping Children Safe in Education and the DFE Filtering & Monitoring Standards, IT Services will ensure compliance is maintained.

3.15.2 All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report any of the following to IT Services immediately.

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material
- they notice the misspelt address diverts them to a phishing login page or similar service

3.15.3 Yeovil College operates an effective filtering system that blocks internet access to harmful sites and inappropriate content. It should not and will not unreasonably impact teaching and learning or college administration. If perceived unreasonable restrictions are observed, please contact IT Services.

3.15.4 IT Services provide and share at minimum, monthly reports and information relating to filtering practices with relevant Designated Safeguarding Leads (DSL) and supporting departments for the purposes of safeguarding and compliance in accordance with Keeping Children Safe in Education (KCSIE).

3.15.5 IT Services have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or system checks

3.15.6 IT Services will perform regular routine testing and updating of the filtering and monitoring systems to ensure their effectiveness. Annual reviews of the filtering and monitoring solutions will be held with the DSL and senior leadership team.

3.15.7 All users are responsible for safeguarding college data and systems by adhering to cybersecurity protocols, staying vigilant against phishing attempts, and promptly reporting any suspicious emails or activities to the IT Services department.

3.15.8 Additional cybersecurity training will be offered to staff who are considered at high risk based on previous interactions with phishing campaigns ran by IT Services.

3.16 Vandalism

3.16.1 Acts of vandalism are taken very seriously. Anyone caught vandalising IT Resources will result in disciplinary proceedings (in line with the Learner Disciplinary Policy for students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff) and/or legal proceedings.

3.16.1 Any costs incurred repairing or replace vandalised equipment will be charged to anyone caught vandalising IT Resources.

3.16.2 To minimise the risk of accidental damage to IT equipment, Food & Drink is not permitted in any Learning Resource area, computer suites, or while working on college IT equipment.

3.16.3 Users are not permitted to unplug or move any non-mobile IT Resources. If the non-mobile IT Resources is required to be moved, please contact IT Services for support.

3.17 Online Etiquette, Offensive Content, Bullying and Harassment

3.17.1 When using IT, all users must uphold the same standards of conduct and behaviour that would be expected at all other times whilst working or studying at the College.

3.17.2 For example, the use of IT to create, share, or distribute offensive content, or to bully or harass others is not permissible, and would result in disciplinary action (in line with the Learner Disciplinary Policy for students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff).

3.17.3 Similarly, the use of IT to attempt to cheat, plagiarise, falsify work, or act in any other way that breaches academic regulations or the principles of academic integrity is not permissible, and

would result in disciplinary action (in line with either the Academic Misconduct Procedure or the Learner Disciplinary Policy for students[4], which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Malpractice and Maladministration Policy[5] or Disciplinary and Grievance Policy for staff).

3.18 Software

3.18.1 Users are not permitted to install software on any IT Resources, including running portable applications.

3.18.1 The installation of software applications can be requested via the IT Helpdesk. All requests must follow the Software Licensing and Management Policy[6] and any cost associated must be agreed and budgeted for, prior to an agreement to purchase.

3.18.2 Cloud based software and services may require a Data Sharing Agreement, where College data is stored externally to the College. This procedure is covered under the Data Protection Policy and must be completed by the system owner.

3.18.3 Use of cloud-based software applications which stores personal information of staff or learners must be approved by the Data Protection Officer and the IT Services Manager.

3.19 Viruses & Malware

3.19.1 Yeovil College uses several layers of security systems to protect data and IT Resources from viruses and malware.

3.19.1 Users must report immediately to the IT Helpdesk if a virus has been identified on an IT Resource. Make sure the IT Resource is turned off and the location is noted to the IT Helpdesk.

3.19.2 Attempts to circumvent any security systems, including Anti-Virus software will result in disciplinary and/or legal action (in line with the Learner Disciplinary Policy for students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff).

[4] Available at https://www.yeovil.ac.uk/policies-reports/
[5] Available at https://www.yeovil.ac.uk/policies-reports/
[6] Available at https://www.yeovil.ac.uk/policies-reports/

3.19.3 Attempts to execute files, scripts or code known to be malicious will result in disciplinary and/or legal action (in line with the Learner Disciplinary Policy for students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff).

3.20 Internet Access

3.20.1 The College internet access is provided via the JANET National network. While using the internet, all Users agree to the JANET Acceptable Use Policy.

3.20.2 Yeovil College's Social Media Policy[7] details acceptable online behaviours and electronic communication and the additional responsibilities which you must accept before accessing Social Media sites.

3.20.3 The College uses a web filtering solution to block access to websites which may contain inappropriate content, non-educational content or present a security concern. Just because the content is not filtered does not mean it is OK to access. If Users feel they have accessed something by mistake which is inappropriate on a college network, please contact the IT helpdesk asap.

3.20.4 All Users must only access web resources where it relates to the academic or business requirement, for educational purposes only.

3.20.5 All Users must not deliberately or knowingly seek to access material that is illegal and/or without proper licensing.

3.20.6 All Users must exercise considerable care and responsibility when browsing the internet, considering search terms that are trying to be accessed.

3.20.7 The College monitors and logs all usage of the Internet.

3.20.8 Downloading or streaming of copyrighted material which is not licenced to view/access, may result in disciplinary or legal action (in line with the Learner Disciplinary Policy for students,

[7] Available at https://www.yeovil.ac.uk/policies-reports/

which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff).

3.20.9 The use of Peer-to-Peer software including BitTorrent is not permitted to run while connected to any Yeovil Colleges networks.

3.20.10 Access to the Dark Web or Tor Networks is not permitted while connected to any Yeovil Colleges networks.

3.20.11 All Users must not connect or tether IT Resources (excluding College IT Laptops) to any other networks or internet connections without approval from IT Services. This will be centrally recorded in IT Services.

3.20.12 College IT Laptop resources should only be connected to secure, password protected home and business Wi-Fi networks.

3.20.13 Misuse of Yeovil Colleges Internet Access or any attempt to circumvent security systems, including web filtering, may result in banned access, disciplinary and/or legal action (in line with the Learner Disciplinary Policy for students, which include steps for referral of matters to the police where conduct may also constitute a criminal offence, or the Disciplinary and Grievance Policy for staff).

3.20.14 Exam user accounts will be removed from having internet access, unless stipulated in the testing process.

3.21 Bring Your Own Device (BYOD) / Personal Devices

3.21.1 **Users** may connect their own devices to the College **Campus** WIFI service, using their **User Account** details. The corporate WIFI (YCWifi) services should not be accessed.

3.21.2 **Users'** Own Devices may be connected by Campus WIFI only. Connecting via Ethernet cable is not permitted under any circumstances.

3.21.3 The activity of **Users'** Own Devices is monitored and logged. Devices may be blocked if in breach of this policy or considered to be a security risk.

3.21.4 IT Services are unable to support **Users'** own devices, including the recovery of data. If experiencing issues, with wireless configuration or joining our WIFI, please contact the IT helpdesk.

3.21.5 Personal Hotspots or Bring Your Own Network (BYON) is not permitted.

3.21.6 Use of anonymizing, VPN or proxy software is not permitted on any of Yeovil Colleges networks.

3.21.7 Own devices are used, connected, and configured at the **Users'** own risk.

3.21.8 BYOD devices must have the latest operating system versions and all critical and important application updates installed within 14 days of release by the manufacturer before connecting to Yeovil colleges systems or data. This is a requirement for Cyber Essentials certification and must be strictly adhered to.

3.21.9 Software designed to log or bypass network security must **not** be connected, stored or ran on the colleges network.

3.21.10 Vintage or obsolete devices which no longer receives updates, must **not** be used to access Yeovil College systems or data.

3.21.11 BYOD devices must be running an un-modified version of the manufactures supported operating system and firmware, Jailbroken or rooted devices must not be used to access Yeovil Colleges systems or data.

3.21.12 BYOD devices must have a timeout password / PIN code set to automatically lock after no longer than 10 minutes of inactivity.

3.21.13 BYOD devices must be configured with separate login profiles where possible, so Yeovil College systems and data are kept away from personal usage.

3.21.14 **Users**' must not try to navigate around security measures put in place by Yeovil College. The CAMPUS WIFI is designed for educational internet services only.

3.21.15 Users who wish to bring their own chargers for personal electronic devices must ensure they are from reputable and quality-tested brands. There have been many reported instances

where dangerous or counterfeit products purchased from online vendors have caused damage to property, equipment, harmed users, or even led to fires.

3.21.16 Any user who wishes to use their personal electronic chargers must ensure that there is no physical damage present, including cracks to the housing, fraying of cables, melting or scorching or any other imperfections not as designed by the manufacturer. If a user is unsure of this, they should not use the product and seek advice from IT Services.

3.21.17 A reputable brand of consumer electronics will have a valid and signed EU Declaration of Conformity for that product. Having a valid and signed EU Declaration of Conformity indicates that the product meets all the necessary requirements of the legislation applicable to the specific product, including usage of the CE marking.

3.21.18 Many products require CE marking before they can be sold in the EU. CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health and environmental protection requirements. It is required for products manufactured anywhere in the world that are then marketed in the EU.

3.21.19 The general principles of the CE marking are contained within Regulation (EC) No 765/2008, which sets the requirements for accreditation relating to the marketing of products.

3.22 Remote Working

3.22.1 While working away from Yeovil College, special considerations must be made by Users working environments, and the people around them, ensuring data and individual security.

3.22.2 Data containing personal or sensitive information must not be taken out of the College unless encrypted and agreed by the systems owner.

3.22.3 Users must assess their environment and position of screens so they cannot be viewed by others.

3.22.4 IT Resources must not be connected to unsecured public WIFI networks.

3.22.5 Further guidance on the use of public WIFI can be found on the NCSC website.

3.22.6 Portable college equipment that has been purchased by IT Services, has remote access to the colleges Domain by prior arrangement only. This equipment utilises the Yeovil College installed VPN service, which should not be tampered with, replicated or changed.

3.22.7 VPN access is not available for personal devices.

3.22.8 Staff are not permitted to access college data and systems from outside of the UK unless authorised to do so by the Principalship team. This includes transporting college devices outside of the UK.

3.22.9 Staff access to college data and systems from outside of the UK must be requested by a member of CLT in writing via the IT Helpdesk. This procedure will be upheld by IT Services as set out in the ITS "Staff Abroad Access Process". This request will be forwarded to the Principalship team for approval.

3.22.10 Student access to college data and systems from outside of the UK must be requested by the students tutor via the agreed process within the Staff Forms Library. Additional checks will be carried out with other relevant college departments e.g. Student Support, prior to approval.

3.23 Loan Equipment

3.23.1 IT Resources may be available for Users to take off-site. IT Services manage all staff loan equipment and learners are managed by the Learning Resource Centre and the iZone team.

3.23.2 A Loan Agreement Form must be signed, agreeing to the terms and conditions of the loan, before any loaned IT Resources are taken off-site. If the user is under the age of 18-year-old, a parent or guardian must sign the Loan Agreement Form before the equipment can be released to the user.

3.23.3 All devices must be collected and returned in person to IT Services; devices will not be issued to anyone else other than the loanee.

3.23.4 Users sign to confirm they have received the loaned IT Resources and it is signed back in when returned.

3.23.5 Directly loaned IT Resources must only be used by the user who it has been configured for and who has signed the Loan Agreement Form.

3.23.6 Loaned IT Resources must not be used by:

3.23.6.1.1 Any member of staff or learner, other than who has signed the Loan Agreement Form.

3.23.6.1.2 Any friends or family member.

3.23.6.1.3 Anyone other than the User who has signed the Loan Agreement Form.

3.23.7 The geographic location of college-owned equipment may be tracked. Loaned equipment is not permitted to be used outside of the United Kingdom, unless where agreed by IT Services.

3.23.8 Users must apply any security updates for loaned IT Resources within 2 working days of being notified an update is available.

3.23.9 Any loaned IT Resources not updated within 3 working days may be disabled and the loaned IT Resources must be returned to the IT Services with the next 5 working days.

3.23.10 IT Services reserve the right request the return of loaned IT Resources at any time.

3.23.11 Loaned IT Resources must be returned to the IT Department within 5 working days of a return is requested.

3.23.12 Loaned IT Resources are vulnerable to theft and must never be left within view of the public including within vehicles. Full details and responsibilities are included in the Loan Agreement Form.

3.23.13 It is recommended that Users check that loaned IT Resources are covered by home and car Insurance policies in the event of theft.

3.23.14 Users may be invoiced for the repair or replacement of any lost or damaged loaned IT Resources, as per the Loan Agreement Form.

3.23.15 Users may be invoiced for any equipment which has not been returned to the IT Helpdesk within 5 days of it being requested.

3.23.16 IT Resources must never be used while driving.

3.23.17 Call, data and message costs are monitored. Users will be charged for excessive personal usage.

3.23.18 The college issued mobile devices are pre-configured with drive encryption to help protect loss of data from theft. Only agreed college mobile apps should be installed on mobile devices, by IT Services.

3.23.19 User is reminded that drive encryption is only effective if the thief does not have access to or cannot obtain or guess the Users password.

3.23.20 PIN codes and passwords must be secured at all times and must not be kept with the device.

3.23.21 If a mobile device has been lost or stolen it must be reported to the IT Helpdesk (01935 845321) immediately.

3.24 Data Security, Removable Media & Backups

3.24.1 Personal & Confidential College information must never be sent or saved to personal accounts or devices.

3.24.2 This includes:

3.24.2.1 Personal email accounts.

3.24.2.2 Personal cloud storage including accounts you have created yourself with your college email address.

3.24.2.3 USB drives, recordable media and personal storage devices.

3.16.2.4 Personal computers, laptops, tablets, phones etc.

3.24.3 Emails, documents & data may be accessed via the mobile apps and web browsers, but personal & confidential information must never be saved to personal devices. If in doubt, please contact helpdesk@yeovil.ac.uk for advice.

3.24.4 Personal & Confidential College information may only be shared with external companies, contractors or individuals where a data-sharing agreement and business contract has been signed by both parties.

3.24.5 Personal & Confidential College information must only be sent to permitted external companies, contractors or individuals using a secure encrypted method of transfer. For advice, please contact the data protection officer or helpdesk@yeovil.ac.uk.

3.24.6 All data must be saved to approved College servers or services. Users should not save files or folders on local desktops.

3.24.7 Backups of Personal & Confidential information by Users is not permitted on college equipment.

3.24.8 All IT Resources must be configured and connected to Yeovil Colleges domain by the IT Services.

3.25 Non-Work-Related Data and Documents

3.25.1 Only data relating to Yeovil College's business are to be saved on college servers, systems or databases.

3.25.2 Private & Personal non-work-related media, data, documents and records must never be saved to any Yeovil College servers, systems or databases.

3.25.3 Yeovil College is not responsible for maintaining the security, retention or any legal requirements of any private or personal non-work-related data stored on college servers or systems or databases.

3.25.4 Yeovil College reserves the rights to delete or prevent access to any private or personal non-work-related data stored on college servers or systems or databases, at any time and without notice.

3.25.5 At the end of employment contracts, Staff are not permitted to transfer any data from college servers, systems or databases without agreement from the HR department.

3.26 IT Resource Requests & Disposal

3.26.1 Additional IT Resources are generally requested at department level, within the annual budget planning process. Agreed budget allocation for IT Resources will be review by the

Head of IT Services, for suitability. Once agreed, the Finance department present a budget code, that IT Services will order the equipment against.

3.26.2 Departments may request IT Resources at their mid-year, flex budget review meeting. Agreed budget allocation for IT Resources will be reviewed by the Head of IT Services, for suitability. Once agreed, the Finance department will present a budget code, that IT Services will order the equipment against.

3.26.3 All IT Resources must be purchased in accordance with the Financial Regulations and Procedures Policy and agreed by the Head of Finance and Head of IT Services.

3.26.4 All IT Resources must be disposed of via IT Services, using a registered IT disposal company with ISO 27001 data security and in accordance with Waste Electrical and Electronic Equipment recycling (WEEE) Directive.

3.26.5 The sale or donation of any Yeovil College IT Resources is not permitted.

3.26.6 Upon request or leaving employment, all IT Resources must be returned in person, to IT Services.

3.26.7 If IT resources need to be reallocated, they must be returned to IT Services first, for reallocation.

3.27 IT Support

3.27.1 All issues/incidents with IT equipment or systems must be reported to IT Services via the helpdesk@yeovil.ac.uk.

3.27.2 All IT issues and requests are logged, prioritised and tracked to resolution.

3.27.3 To log an IT support call, Users will be asked for the computer name, location, login name and a detailed description of the problem.

3.27.4 All criminal incidents will be reported for legal investigation.

4. RESPONSIBILITIES

4.1 Compliance, Monitoring and Review

4.1.1 Yeovil College Governing Body is responsible for:

4.1.1.1 Approval of this policy.

4.1.2 Yeovil College Senior Management Team (SLT) is responsible for:

4.1.2.1.1 Recommending approval of policy to the governing body.

4.1.2.1.2 Ensure this policy reinforces the strategic objectives of the College.

4.1.3 IT Services Manager is responsible for:

4.1.3.1.1 Ensuring this policy meets legal & regulatory requirements.

4.1.3.1.2 Ensuring a robust, risk-based approach to cybersecurity.

4.1.3.1.3 Ensuring a flexible approach to IT delivery.

4.1.3.1.4 Investigating any breach of policy, with the relevant department support.

4.1.3.1.5 Reporting any IT related concerns to the business or curriculum VP's.

4.1.4 All Information Users are responsible for:

4.1.4.1.1 Ensuring compliance with this policy.

4.1.4.1.2 Understand their responsibilities concerning the use of IT Resources.

4.1.4.1.3 Reporting suspected breaches of this policy to IT Services for investigation.

4.2 Reporting

4.2.1 No additional reporting is required.

5. RELATED LEGISLATION AND DOCUMENTS

5.1 Legislation

Users are responsible for complying with all legal requirements while using the Colleges IT Resources including but not limited to:

- The Computer Misuse Act 1990
- The Data Protection Act 2018
- The Obscene Publications Act 1959
- The Copyright, Designs and Patents Act 1988

- The Regulation of Investigatory Powers Act 2000
- The Communications Act 2003
- The Digital Economy Act 2010
- The Malicious Communication Act 1988
- Counter Terrorism and Security Act (2015)

5.2 Other Policies & Procedures[8]

- Data Protection Policy
- Data Sharing Agreement.
- Learner Disciplinary Procedure.
- Student Code of Conduct.
- Code of Professional Standards.
- Disciplinary Policy and Procedure.
- Software Licensing & Management Policy.
- Safeguarding Policy and Procedure.
- Keeping Children Safe in Education (Department for Education 2 September 2024).
- Filtering & Monitoring Standards for schools and colleges (Department for Education 22 Oct 2024)
- Searching, screening and confiscation in schools (Department for Education July 2023).
- Prevent duty guidance: England and Wales (2023)

5.3 3rd Party Policies, Procedures, Terms & Conditions

Users are responsible for complying with all agreements/terms and conditions while using IT resources including but not limited to:

- Jisc Acceptable Use Policy.
- Software / Website Licence Agreements.
- Software / Website Terms & Conditions.
- Copyright Agreements.

6. DEFINITIONS

6.1 Terms and definitions

[8] College policies and procedures are available at https://www.yeovil.ac.uk/policies-reports/, with the exception of the Code of Professional Standards and the Disciplinary and Grievance Policy for staff which are available to Yeovil College staff via the Policies and Procedures section in the College SharePoint.

6.2 **BYOD:** Bring Your Own Device, A term used for using personally owned devices to access Yeovil Colleges systems and data.

6.2 **Information Assets:** Any form of information, document or data which has a value to Yeovil College.

6.4 **Information Security:** Protecting against the unauthorized use of Information Assets Information Users: Any members of staff, learner, associate, partner and stakeholder who interact with Yeovil Colleges Information Assets.

6.5 **IT Helpdesk –** IT Services support desk 01935 845321 | helpdesk@yeovil.ac.uk. Supporting IT Resources – include College computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, IT peripherals, software, cloud services, IT systems, Access to WIFI, etc.

6.6 **IT Services –** 01935 845321 | helpdesk@yeovil.ac.uk. IT Resources – include College computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, IT peripherals, software, cloud services, IT systems, Access to WIFI, etc.

6.7 **IT Resources:** Includes Computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, equipment, software, services, systems, Access to WIFI, etc.

6.8 **Multi-Factor Authentication (MFA):** A code sent to mobile by SMS message or via an App which is required to login as well as your password.

6.9 **User Account:** Username & Password used to login to the Yeovil Colleges network.

6.10 **Users:** Enrolled learners, members of staff and associates.

APPENDIX A - Student Guidance: Using IT Appropriately at Yeovil College

Using IT Appropriately at Yeovil College

There are rules that Yeovil College expects all students to follow to ensure they are using technology appropriately during their learning. Key rules are outlined below, and the College's 'Acceptable Use of IT Policy' sets out these rules in more detail. It is important that students read and understand these rules. Failure to follow these rules would result in a range of disciplinary consequences, including under the Learner Disciplinary Policy, the Academic Misconduct Procedure, or potential legal action or criminal proceedings if a student's misuse of IT also constitutes a criminal act.

THESE RULES APPLY TO:

- All students whilst at College, no matter whether they are using a College device or their own.
- All students undertaking College activity off-site (e.g. a trip, or learning in the workplace), no matter whether they are using a College device or their own.
- All students using a College device or accessing the College network, at any time, no matter where they do this from.

STUDENTS MUST

- Keep their user information, including their password, safe at all times. This information shouldn't be shared with others.
- Treat equipment and the College IT network with respect.
- Use IT responsibly to support their learning, as directed by their teachers. (E.g. students should not be on Social Media in lessons when they're meant to be working on tasks or taking notes).
- Inform a member of staff immediately if they accidentally access unsuitable material, believe their account has been compromised, or are concerned by something they have seen or experienced.
- Be aware that College keeps logs of all software usage and websites visited using College systems (including College WiFi), as well as emails and messages sent and received using College systems.
- Read the Acceptable Use of IT Policy for full details of what is and is not acceptable behaviour.

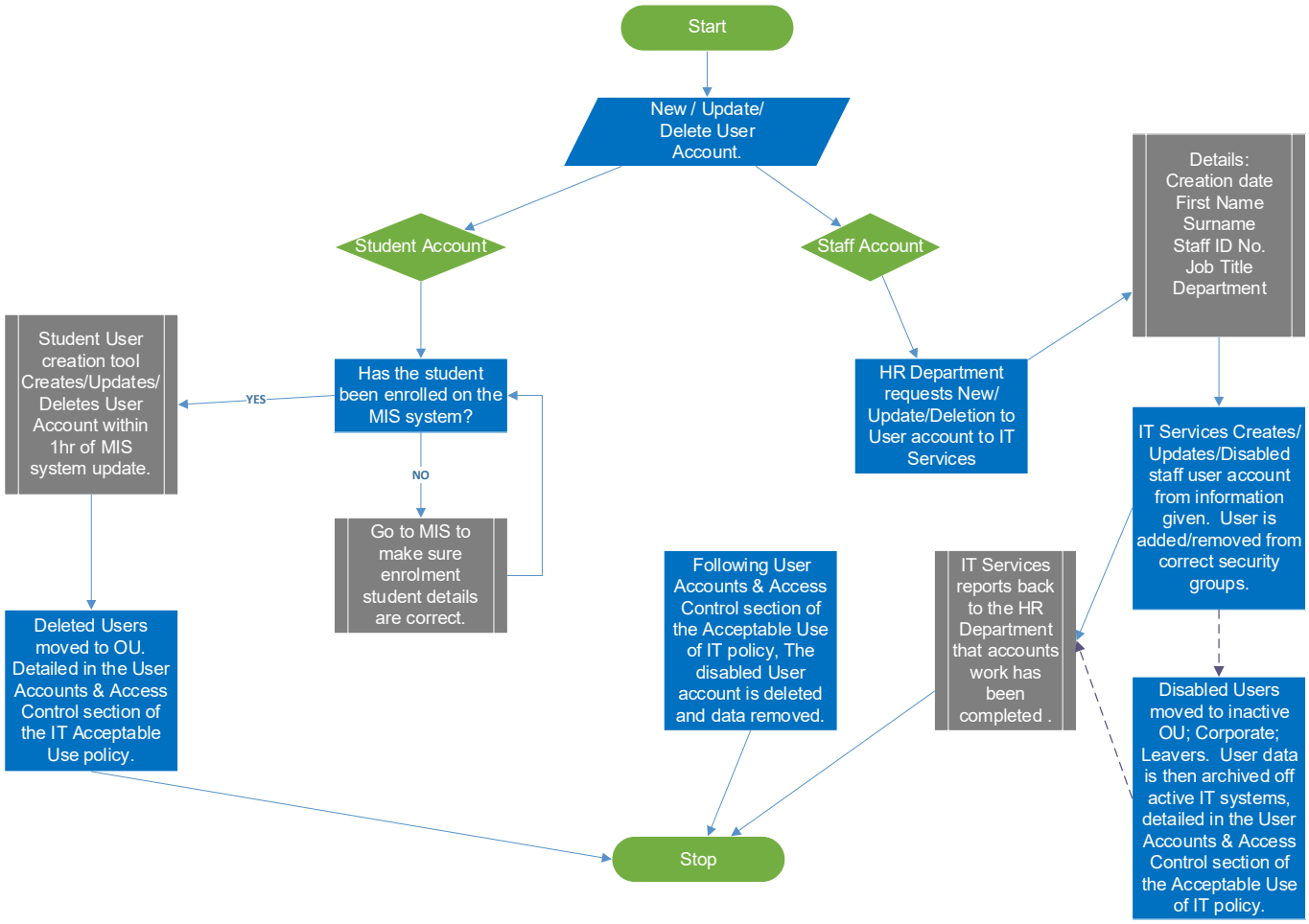
STUDENTS MUST NOT

- Access, share or create inappropriate material, including things that could offend other people.
- Take pictures or record other people without their permission.
- Use a device that is logged on by someone else, nor interfere with someone else's files or account.

- Harass or bully other people.
- Use College systems to store personal files or run a private business.
- Deliberately try to bypass College filters or safeguards, nor attempt to download or install other programmes onto a College device.

APPENDIX B - Account Creation / Update / Deletion Process

Staff and Learner Account Creation / Updates / Deletion Process



APPENDIX C - Complex Password Rules

Complex Password Rules

The following rules apply to all **User Account** passwords:

- A minimum of 12 characters long.
- Must not contain the User's: First, Middle or Last Names.
- Must not have been used in the last 5 passwords history. i.e. old passwords that you've used before.
- Must contain the following characters from following categories:
  1. Uppercase characters of European languages (A through Z)
  2. Lowercase characters of European languages (a through z)
  3. Base 10 digits (0 through 9)

It is also recommended to use:

4. Non-alphanumeric characters: ~!@#$%^&* -+=`|\(){}[]:;'"<>,.?/
5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.