Reference Number: *P32*

YEOVIL COLLEGE ACCEPTABLE USE OF IT POLICY

Policy Review				
Author Craig Cullen	Position Head of Infrastructure	Approved by SMT Signed:	Approval date 26/9/22	Review date Sept 23

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		

Initial Equality Impact Screening

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

Yes:
Karen Foster - Head of Resource Innovation
Michelle Joy - Head of Student Experience
Sian Deasy - HE Manager

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

Review of the existing student and staff acceptable use policy to rewrite policy, including newly implemented IT systems.

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:	**Craig Cullen**	**Position:**	**Head of Infrastructure**	**Date:**	**26/09/22**

□ Reviewed by Equality & Diversity Group: YES/NO If Yes: Date:

□ I confirm that any recommended amendments have been made

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

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

CONTENTS

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.

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

User Accounts & Access Control

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

3.2 Attempting to create, circumvent or elevate permissions of Users Accounts by any other method will result in disciplinary or legal action.

3.3 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.

3.4 Attempting to obtain another User Account's details by any method will result in disciplinary or legal action.

3.5 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.

User Account Creation

3.6 Staff Accounts

- Line Managers must request User Accounts for staff via the Human Resources (HR) department. IT Services will only create, change, or delete accounts, under the direction of the HR department.
- Appendix A shows the staff account creation process.

3.7 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.

User Account Removal

3.8 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 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.

3.9 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.

Guest / Generic Accounts

3.10 IT Services may provide Guest / Generic User accounts. This is under the discretion of IT Services, who will assess security concerns before the creation of an account. Guest or generic 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.

3.11 All user accounts must be associated with an individual, except where approved by the senior IT Services team. In that case, the user account will be associated to a department.

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

Administration Accounts

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

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

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

Access Control

3.16 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.

3.17 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).

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

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

Passwords & Authentication

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

- 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.

- 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 3 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.

3.21 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.

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

<u>Reduce Reliance on passwords</u>

3.23 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).

<u>MFA or Two Factor Authentication (2FA)</u>

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

3.25 Users will be required to register a personal device such as a mobile phone, to confirm their identity against MFA or 2FA logins.

3.26 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.

3.27 In cases where users do not have access to a mobile phone, they should contact IT Services to request a solution.

Password Managers

3.28 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.

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

3.30 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.

Communication Systems

3.31 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.

3.32 Full details are covered under the communications policy.

Data Security

3.33 To ensure data security, the College has a clear screen & desk policy.
This means:

- Users must lock the PCs EVERY TIME they leave their computer or desk, even if it is only for a short period.
- All printed documents with personal information must be kept in a locked draw or cabinet EVERY TIME Users leave their desk.
- Passwords must never be shared. If someone else needs access to documents, emails, systems etc. Users must contact the IT Helpdesk for advice.
- 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.

3.34 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 for more details.

Monitoring and Logging

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

3.36 Monitoring and logging include:

- Login / logout.

- Location login / logout
- File activity.
- Internet activity.
- Communication.
- Location tracking of equipment.
- Screen capture or monitoring.

3.37 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.

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

Safeguarding and Prevent

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

- The information which may lead to potential terrorism or extremist activity such as sites categorised as:
  - Intolerance
  - Personal Weapons
  - Terrorism
  - Violence
- The information which may lead to a potential risk to young people or vulnerable adult's Internet activity including sites categorised as:
  - Adult entertainers
  - Adult sites
  - Child abuse
  - Pornography
  - Restricted to adults
  - Anonymous chat websites

3.40 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.

Vandalism

3.41 Acts of vandalism are taken very seriously. Anyone caught vandalising IT Resources will result in disciplinary and/or legal proceedings.

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

3.43 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.

3.44 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.

Software

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

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

3.47 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.

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

Viruses & Malware

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

3.50 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.

3.51 Attempts to circumvent any security systems, including Anti-Virus software will result in disciplinary and/or legal action.

3.52 Attempts to execute files, scripts or code known to be malicious will result in disciplinary and/or legal action.

Internet Access

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

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

3.55 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.

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

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

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

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

3.60 Downloading or streaming of copyrighted material which is not licenced to view/access, may result in disciplinary or legal action.

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

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

3.63 All Users must not connect or tether to any IT Resources to any other networks or internet connections without written approval from the IT Services.

3.64 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.

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

Bring Your Own Device (BYOD) / Personal Devices

3.66 **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.

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

3.68 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.

3.69 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.

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

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

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

3.73 BYOD devices must have the latest operating system and application updates installed before connecting to Yeovil colleges systems or data. Software designed to log or bypass network security must **not** be connected to the colleges network.

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

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

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

3.77 BYOD devices must be configured with separate login profiles, so Yeovil College systems and data are kept away from.

3.78 **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.

Working from Home

3.79 While working away from the Yeovil College, special considerations must be made by Users working environment and the people around you, ensuring data and individual security.

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

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

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

- Further guidance on the use of public WIFI is available from the NCSC website.

3.82 Portable college equipment that has been purchased by IT Services, has remote access to the colleges Domain. This utilises the Colleges installed VPN service, which should not be tampered with, or changed.

3.83 Remote access is also available on the Remote Desktop service for business support departments only. This utilises MFA for additional security at user log on.

3.84 VPN access is not available for personal devices.

3.85 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 from outside of the office.

- College mobile phones will not be issued for specifically for MFA purposes. In some special cases, users do not have access to a personal device. Please contact IT Services for a possible loaned equipment to support this security requirement. This is a token key that will be able to give a unique passcode.

Loan Equipment

3.86 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.

3.87 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.

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

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

3.90 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.

3.91 Loaned IT Resources must not be used by:

- Any member of staff or learner, other than who has signed the Loan Agreement Form.
- Any friends or family member.
- Anyone other than the User who has signed the Loan Agreement Form.

3.92 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.

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

3.94 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.

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

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

3.97 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.

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

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

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

3.101 IT Resources must never be used while driving.

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

3.103 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.

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

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

Data Security, Removable Media & Backups

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

This includes:

- Personal email accounts.
- Personal cloud including accounts you have created yourself with your college email address.
- USB drives, recordable media and personal storage devices.
- Personal computers, laptops, tablets, phones etc.

3.106 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.

3.107 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.

3.108 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.

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

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

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

Non-Work-Related Data and Documents

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

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

3.114 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.

3.115 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.

3.116 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.

IT Resource Requests & Disposal

3.117 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.

3.118 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.

3.119 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.

3.120 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.

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

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

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

IT Support

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

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

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

3.127 All criminal incidents will be reported for legal investigation.

4 RESPONSIBILITIES

Compliance, Monitoring and Review

4.1 Yeovil College Governing Body is responsible for:

- Approval of this policy.

4.2 Yeovil College Senior Management Team (SMT) is responsible for:

- Recommending approval of policy to the governing body.
- Ensure this policy reinforces the strategic objectives of the College.

4.3 Head of IT is responsible for:

- Ensuring this policy meets legal & regulatory requirements.
- Ensuring a robust, risk-based approach to cybersecurity.
- Ensuring a flexible approach to IT delivery.
- Investigating any breach of policy, with the relevant department support.
- Reporting any IT related concerns to the business or curriculum VP's.

4.4 All Information Users are responsible for:

- Ensuring compliance with this policy.
- Understand their responsibilities concerning the use of IT Resources.
- Reporting suspected breaches of this policy to IT Services for investigation.

Reporting

4.5 No additional reporting is required.

5 RELATED LEGISLATION AND DOCUMENTS

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)

Other Policies & Procedures

- Data Protection Policy
- Data Sharing Agreement.
- Student 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 3 September 2018).
- Searching, screening and confiscation (Department for Education January 2018).

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

Terms and definitions

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

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

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.

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.

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.

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

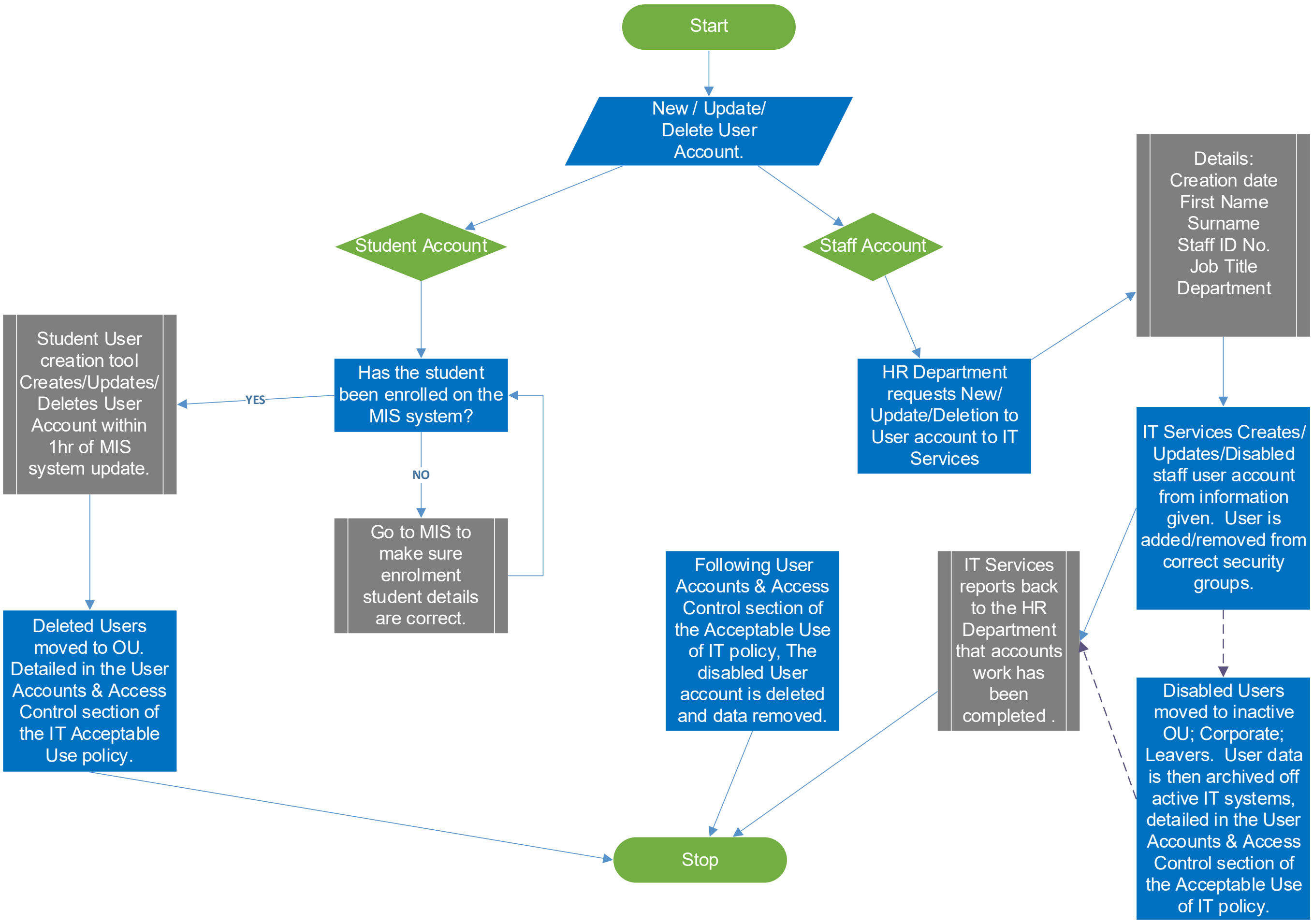
Multi-Factor Authentication (MFA): A code sent to mobile by SMS message or via an App which is required to login as well as your password.

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

Users: Enrolled learners, members of staff and associates.

7. APPENDIX A

Staff and Learner Account Creation / Updates / Deletion Process


Start
New / Update/ Delete User Account.
Student Account
Staff Account
Details: Creation date First Name Surname Staff ID No. Job Title Department
Student User creation tool Creates/Updates/ Deletes User Account within 1hr of MIS system update.
YES
Has the student been enrolled on the MIS system?
NO
HR Department requests New/ Update/Deletion to User account to IT Services
IT Services Creates/ Updates/Disabled staff user account from information given. User is added/removed from correct security groups.
Go to MIS to make sure enrolment student details are correct.
Following User Accounts & Access Control section of the Acceptable Use of IT policy, The disabled User account is deleted and data removed.
IT Services reports back to the HR Department that accounts work has been completed .
Deleted Users moved to OU. Detailed in the User Accounts & Access Control section of the IT Acceptable Use policy.
Disabled Users moved to inactive OU; Corporate; Leavers. User data is then archived off active IT systems, detailed in the User Accounts & Access Control section of the Acceptable Use of IT policy.
Stop

8. APPENDIX B

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 be changed every 90 days.
- 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.