Weston College Group

IT ACCEPTABLE USE POLICY

IT ACCEPTABLE USE POLICY

CONTENTS

Change Control

Date approved by CLB:	February 2025 - TBC
Date approved by Corporation:	February 2025 - TBC
Name of policy holder:	Matt Beaver
Date issued:	February 2025
Review date:	January 2026

Review Date	**Changes**
February 2025	• Improvements to the wording and clarity throughout the document • Updated Purpose & Scope statement to improve clarity and align with the IT Security Policy • Updated Terms and Definitions • Added an AI in Meetings section • Added a Use Personal Device and Services section • Updated user account creation process, included learner exam accounts

IT ACCEPTABLE USE POLICY

1 PURPOSE

1.1 The purpose of this IT Acceptable Use Policy is to establish guidelines for the secure and responsible use of Weston College Group's IT systems & resources.

1.2 This policy aims to safeguard personal and sensitive information by outlining clear policies on data handling, storage, and sharing, thereby protecting the privacy and integrity of all users' data.

1.3 To ensure compliance with relevant legislation and regulatory requirements, including data protection laws and IT security standards, thereby mitigating legal and reputational risks.

1.4 To promote the efficient and effective use of IT resources, ensuring that all users understand their responsibilities and the procedures for accessing, using, and maintaining IT systems and services.

2 SCOPE

2.1 This policy applies to anyone who uses the Weston College network, IT resources, systems, or resources. This includes, but is not limited to, all staff, students, contractors, visitors, and any other individuals or entities granted access to the College's IT infrastructure.

2.2 The policy covers all aspects of IT usage, including hardware, software, data, and communication systems, regardless of the location from which they are accessed.

2.3 It ensures that all users adhere to the security protocols and procedures necessary to protect the confidentiality, integrity, and availability of the College's information assets.

2.4 Compliance with this policy is mandatory for all users to maintain a secure and resilient IT environment.

3 ACCESS CONTROL POLICY

3.1 Access to Weston College Group IT resources is granted through a user account assigned to an individual named user.

3.2 Any attempt to create, circumvent, or elevate permissions of user accounts will result in disciplinary and/or legal action.

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

3.4 Any attempt to obtain another user's account details by any method will result in disciplinary and/or legal action.

3.5 Staff may be required to assist learners with user account details; this must only be done with the learner's consent each time it is required.

User Account Creation

<u>Staff Accounts</u>

3.6 Line managers must request user accounts for staff via the New User Request Form on SharePoint.

3.7 Appendix A details the staff account creation process.

Tutor Accounts (t. Accounts)

3.8 Tutor user accounts (t. Accounts) will be automatically created at the same time as staff accounts.

3.9 Appendix A details the staff account creation process.

Learner User Accounts

3.10 Learner user accounts will be automatically created overnight when there is an active application or enrollment in the Learner Management System (LMS).

Learner Exams Accounts

3.11 Learner exam user accounts will be automatically created overnight following the creation of the learner user accounts.

User Account Removal

Staff Accounts

3.12 Staff user accounts will be automatically deactivated on the end date of their contract.

Tutor Accounts (t. Accounts)

3.13 Tutor user accounts (t. Accounts) will be deactivated at the same time staff as accounts.

Learners Accounts

3.14 Learner user accounts can be disabled at any time by a lead welfare or safeguarding manager contacting the IT Helpdesk.

3.15 All non-active learner user accounts will be automatically disabled upon the completion of their course.

Learners Exam Accounts

3.16 Learner exam user accounts will be disabled at the same time as learner user accounts.

Guest / Generic Accounts

3.17 Weston College does not provide guest or generic user accounts.

3.18 All user accounts must be associated with a named individual, except where approved by the Head of IT.

3.19 Guest Wi-Fi is available for visitors; please refer to the BYOD section for more information.

Privileged Access (Administration Accounts)

3.20 Privileged Access (Administration Accounts) to the domain and local computers are restricted to members of the IT Department.

3.21 Privileged Access (Administration Accounts) to systems and applications will only be granted with the system owner's approval.

3.22 The number of user accounts assigned privileged access (administration accounts) will typically be limited to five user accounts per system.

3.23 Privileged access (administration accounts) group membership will be monitored and reviewed annually.

Access Control

3.24 Access to systems and IT resources is restricted by permissions. To request additional access, please contact the system owner or IT Helpdesk for guidance.

3.25 Access to systems and IT resources may be removed by system owners, the HR department, or a member of the Executive Team at any time by contacting the IT Helpdesk.

3.26 All requests for permission changes must be submitted by email. An IT Helpdesk call will be raised for all permission changes as an audit record.

3.27 The IT Department regularly monitors file access permissions following the process shown in Appendix B.

Passwords & Authentication

3.28 All user accounts will have a complex password/PIN, details of the complex password requirements are detailed in Appendix C

3.29 Users are responsible for all activities that occur while logged in using their user account.

3.30 User accounts will automatically be locked out after five incorrect password attempts.

3.31 Passwords must remain strictly confidential and should never be written down or disclosed to anyone.

3.32 Passwords must never be shared. If someone else knows your password, please change it immediately. If someone else needs access to documents, emails, systems, etc., please contact the IT Helpdesk for advice.

3.33 Passwords may be changed at any time. Please contact the IT Helpdesk for further assistance or advice on passwords.

3.34 User accounts are set to automatically lock after ten minutes of inactivity but must be locked every time you step away from your computer.

3.35 A password manager is a secure web browser plugin that helps generate, store, and enter strong, unique passwords. Weston College supports a number of password management plugins. Please contact the IT Helpdesk for more information.

3.36 Single Sign-On (SSO) is used where available to reduce the number of passwords users are required to remember and enter.

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

3.38 The NCSC Password Policy Infographic explains how passwords are discovered and how system security policies can help.

Multi-Factor Authentication (MFA)

3.39 Multi-Factor Authentication (MFA), also referred to as Two-Factor Authentication (2FA), is used to enhance the security of Weston College user accounts.

3.40 Users will be required to register a personal device, which will be used to confirm their identity.

4 DATA SECURITY

Clear Desk & Clear Screen Policy

4.1 A clear desk and clear screen policy is used to ensure sensitive information is securely stored and screens are locked when not in use, maintaining a tidy workspace and protecting confidential data.

4.2 IT resources must be locked every time a user leaves a computer or desk, even if it is only for a short period.

4.3 All printed documents containing Personally Identifiable Information (PII) or sensitive information must be kept in a locked drawer or cabinet every time a user leaves the desk.

Use of Personal Devices and Services

4.4 Personally Identifiable Information (PII) or information classified as internal or confidential must never be sent or saved to personal cloud accounts, devices, or removable media.

This includes:

- Email accounts that have not been created by the Weston College IT Department.
- Personal cloud accounts (including accounts you have created yourself with your College email address)
- Removable Media, USB drives, recordable media or personal storage devices
- Personal computers, laptops, tablets, phones etc…

4.5 Information assets containing Personally Identifiable Information (PII) and information classified as internal or confidential must never be taken, copied, or downloaded onto personal computers or systems outside of the College's network. Please refer to the Information Security Management System Policy for more details.

4.6 Emails and information assets may be accessed through mobile applications and web browsers. However, Personally Identifiable Information (PII) and data classified as internal or confidential must not be stored on personal devices. If you are uncertain, please contact the IT Helpdesk at it.helpdesk@weston.ac.uk for guidance.

4.7 Personally Identifiable Information (PII) and information classified as internal may only be shared with external companies, contractors or individuals where a Data Sharing Agreement (DSA) has been signed by both parties.

4.8 All Information Assets must be saved to approved College servers or College cloud services.

4.9 Backups of data containing Personally Identifiable Information (PII) or information classified as internal or confidential by users is not permitted.

4.10 All College IT resources must be configured and connected to a College domain by the IT Department.

Private (Non work related) Data and Documents

4.11 Only Information Assets relating to the College business are to be saved on College servers, systems or databases.

4.12 Private (Non work related) media, data, documents and records must not be saved to any College servers, systems or databases.

4.13 The College does not take any responsibly for maintaining the security, retention, or any legal requirements of any Private (Non work related) data stored on its servers, systems, or databases.

4.14 The College reserves the right to delete or prevent access to any private (non work-related) data stored on College servers, systems, or databases at any time and without notice.

4.15 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.

5 DATA PRIVACY

Monitoring & Logging of IT Systems and Messages

5.1 All IT usage and messages are monitored and logged to ensure the security of our systems, maintain compliance with regulatory requirements, and protect the integrity of our IT infrastructure. This helps us detect and prevent unauthorised access, misuse, or breaches, ensuring a safe and reliable environment for all users.

5.2 The list below provides an unexhaustive list of the types of data and messages that are monitored:

- Documents, Files & Database Access
- Geographical Locations of Devices
- Internet activities
- Login activities
- Messages (including Emails & Teams messages)
- Screen captures

5.3 When deemed appropriate and approved by a member of the Colleges Executive Team, data logs and messages will be securely shared with agencies and authorities to assist in their investigations.

5.4 Members of the Executive Team reserve the right to review and monitor any data or messages held on Weston College systems and devices. These requests will be recorded by the IT Department for audit purposes

5.5 Individuals rights to personal information will be processed in accordance with UK privacy laws and our Data Protection Policy

5.6 All data is processed in accordance with our Privacy Notice(s) available from www.weston.ac.uk/dataprivacy

Purposes for Logging and Monitoring IT Systems

5.7 IT systems usage is monitored by the IT Department to investigate and resolve the following:

- Cyber security concerns
- IT performance & reliablity concerns
- The utilisation of resources

Purpose for Monitoring Internet Activity

5.8 Internet activity is monitored and access to websites categorised as high risk are blocked.

5.9 All internet activity is logged and monitored for the following purposes, which will be reviewed exclusively by the teams identified in the table below:

Purpose	**Reviewer(s)**
To identify a **Safeguarding** concern	Safeguarding Team
To identify a **Prevent** concern	Safeguarding Team
To identify a **Cyber Security** concern	IT Department
To identify a **Legal or Reputational** concern	IT Department / Chief Operating Officer
To identify an **Operational Disruption** or **Commercial Threat** concern	Chief Operating Officer

5.10 At times it may also be necessary to block or restrict internet activity for IT performance purposes

Purposes for Monitoring Messages

5.11 Messages (including emails and Teams) will only be monitored for the following purposes and reviewed exclusively by the teams identified in the table below:

Purposes	**Reviewer(s)**
To identify a **Safeguarding** concern	Safeguarding Team
To identify a **Prevent** concern	Safeguarding Team
To identify a **Student Welfare** concern	Student Welfare Team
To identify a **Staff Welfare** concern	Staff Welfare Team / HR Department
To identify a **Cyber Security** concern	IT Department
To identify a **Legal, or Reputational** concern	IT Department / Chief Operating Officer
To identify an **Operational Disruption** or **Commercial Threat** concern	Chief Operating Officer
Where a concern is **reported by a user**	IT Department / HR Department

5.12 As system administrators, the IT Department has access to all data and messages held on Weston College systems but will only process data for the purposes defined above.

Data Loss Prevention (DLP)

5.13 Data Loss Prevention (DLP) is a security approach used to detect and prevent the unauthorised sharing, transfer, or use of sensitive data.

5.14 The College uses Data Loss Prevention (DLP) to scan messages and automatically encrypt any Personally Identifiable Information (PII) detected to help reduce data breaches. This helps ensure compliance with regulatory requirements and contractual obligations by enhancing overall data security through monitoring and controlling data transfers.

Recording Meetings and Conversations

5.15 The recording of meetings and conversations creates a record of decisions and actions, enhancing accountability and tracking progress, ultimately improving communication, collaboration, and productivity within the organisation.

5.16 The College encourages the recording and sharing of meetings to promote:

- accurate documentation of all details discussed,
- allowing participants to revisit the conversation for clarity and reference.
- helps those who couldn't attend stay informed,
- promotes inclusivity,
- resource for training and development.

5.17 Before recording a meeting or conversation, all participants must be informed and give their consent to the recording.

5.18 The purpose of the recording and its intended recipients must be clearly explained to all participants.

5.19 All recordings must be stored securely and used or shared only as described.

5.20 All recordings must be securely deleted when no longer required, such as after the minutes have been written.

Artificial Intelligence (AI) in Meetings

5.21 Only Artificial Intelligence (AI) software approved by the Head of IT may be invited to meetings or used to process meeting or conversation data.

5.22 When AI software is approved for meeting processing, all the controls described above for recording a meeting and conversation must be followed.

6 PHYSICAL SECURITY

Vandalism

6.1 Acts of vandalism are taken very seriously. Anyone caught vandalising IT resources will face disciplinary and/or legal proceedings.

6.2 Any costs incurred from repairing or replacing equipment will be charged to users caught vandalising IT resources.

6.3 To minimise the risk of accidental damage to IT resources, food and drink are not permitted in any computer suites.

6.4 Any damaged IT resources must be reported to the IT Helpdesk as soon as possible.

6.5 Users are not permitted to unplug or move any non-mobile IT resources. If IT resources need to be relocated, please contact the IT Helpdesk to arrange a relocation survey.

7 SOFTWARE

7.1 The term software refers to programs that operate computers and execute specific tasks, encompassing all license types such as public domain, permissive, copyleft, proprietary, freeware, shareware, open source, enterprise, and user licensing.

7.2 Users are prohibited from installing software on any IT resources this includes the execution of portable applications.

7.3 Requests for the installation of software applications must be submitted through the IT Helpdesk.

7.4 Verifiable evidence of the legal right to use software is required prior to its installation. Software will be removed once the evidence of the legal right to use it expires.

7.5 Software will only be installed if there is verifiable evidence of vendor support, including regular updates or patches. The vendor must provide a future date for when they will cease providing updates. Software will be removed if this support can no longer be verified.

7.6 The use of cloud-based software applications that store personal information of learners or staff must be approved by the IT Department.

8 MALWARE AND CYBER THREATS

8.1 Data and IT resources are protected from cyber threats, such as viruses and malware, through the use of a multi-layered security system.

8.2 Users must report to the IT Helpdesk if a computer virus is identified.

8.3 Attempts to circumvent any security systems will result in disciplinary and/or legal action.

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

9 INTERNET ACCESS

9.1 Internet access is provided via the JANET National network. While using the internet all users must agree to terms of the JANET Acceptable Use Policy.

9.2 The E-Safety & Social Media Policy details acceptable online Behaviours and electronic communication, as well as the additional responsibilities you must accept before accessing social media sites.

9.3 Web filtering is used to block websites that may have inappropriate or non-educational content or present security concerns. It is important to note that just because content is not filtered, it does not mean it is appropriate to access.

9.4 Misuse of internet access or attempts to bypass security systems, including web filtering, may lead to disciplinary and/or legal action.

Safeguarding and Prevent

9.5 The College actively monitors and logs the following harmful and unacceptable activities as part of its responsibility towards multi-agency safeguarding, Prevent, and sexual abuse prevention agendas.

- Information that may indicate potential terrorism or extremist activity.
    - Internet activity including sites categorised as:

        - Extremism - *curated by the Counter Terrorism Internet Referral Unit (CTIRU)*

- Information that may identify harmful sexual Behaviour posing a potential risk to young people or vulnerable adults.
    - Internet activity including sites categorised as:
        - Adult
        - Adult Questionable – *a list of URLs from the Internet Watch Foundation (IWF)*

9.6 Logs and information relating to safeguarding, Prevent, or Behaviours indicating sexual harassment will be shared with the College's trained Safeguarding/Prevent officer and may be shared with local authorities for further investigation.

Examples of Unacceptable Internet Usage

9.7 This is an unexhastive list of examples of unacceptable internet usage any of the following may result in disciplinary and/or legal action.

9.8 Any action that contravenes the Computer Misuse Act 1990.

9.9 Accessing any indecent or offensive materials deemed inappropriate within a Further Education environment.

9.10 Deliberately introducing viruses, malware, or other harmful software, scripts or code into the network.

9.11 Attempting to access restricted areas of any network, systems, or data without proper authorisation.

9.12 Downloading or streaming copyrighted material without proper licensing.

9.13 Engaging in harassment, bullying, or threatening Behaviour towards others online.

9.14 Sharing confidential or sensitive information without authorisation, which could compromise the security and privacy of the College.

9.15 The use of Peer-to-Peer (P2P) software, including BitTorrent, is prohibited while connected to any College network, including WIFI networks.

9.16 Accessing the Dark Web or using Tor browsers is prohibited while connected to any College networks, including WIFI networks.

9.17 Users must not connect or tether IT resources to unsupported networks or internet connections without written approval from the IT Department.

Internet Access for Higher Education

9.18 Users accessing content for purposes related to Higher Education (HE) programmes will be granted access to a wider range of websites. However, the following applies:

9.19 The examples of unacceptable internet usage listed above still apply to Higher Education (HE) users including staff.

9.20 Higher Education (HE) users, including staff, must only access resources that are connected with the academic requirements of the HE programme and are for educational purposes only.

9.21 Higher Education (HE) users, including staff, must exercise considerable care when accessing material that some people may find offensive. For safeguarding purposes, if children or vulnerable adults are present, the Further Education (FE) IT Policy applies.

10 MOBILE DEVICE POLICY

Bring Your Own Device (BYOD)

10.1 Learners may connect their own devices to the College Guest WIFI using “eduroam” and their user account details. Users must agree to the **eduroam UK policy** to use this service.

10.2 Where staff are included within the Weston Technical Education network, users' BYOD devices will be blocked from accessing any College systems.

10.3 Users’ BYOD devices may be connected via WIFI only; connecting via Ethernet cable is not permitted.

10.4 The activity of users’ own devices will be monitored and logged. Devices may be blocked without notice if they breach this policy or are considered a security risk.

10.5 IT support services are unable to support users’ own devices, including data recovery. If you experience issues with your BYOD device, please use IT resources supplied by the College.

10.6 The installation of drivers or software in College IT resources to support personal devices will not be permitted.

10.7 Personal hotspots or Bring Your Own Network (BYON) are not permitted unless agreed with the Head of IT.

10.8 The use of anonymising, VPN, or proxy software is not permitted on any College networks including WIFI.

10.9 BYOD devices are used, connected, and configured at the users' own risk.

10.10 The following best practices are recommended for users connecting a BYOD device to Weston College systems:

10.10.1 BYOD devices should be currently supported by the manufacturer and have the latest system/firmware updates installed.

10.10.2 BYOD devices should run a currently supported operating system that has the latest updates installed.

10.10.3 BYOD devices should only have currently supported applications with the latest updates installed

10.10.4 BYOD devices should be running up to date currently supported anti-malware Software which is updated daily and set to automatically scan files and web pages on access and warn of malicious detections

10.10.5 BYOD devices should be running an unmodified version of the manufactures supported operating system and applications, Jailbroken operating systems and applications are not permitted.

10.10.6 BYOD devices should have a timeout password / PIN code set to automatically lock after no longer than 10 minutes of inactivity, Refer to Appendix D for password recommendations

10.10.7 BYOD devices should have all default and easy to guess passwords changed to a strong password, Refer to Appendix D for password recommendations

10.10.8 BYOD devices that are shared with family and friends and used to access Weston College systems should be configured with separate login “profiles” so Weston College systems and data are not available to other users. Any unused user accounts or profiles should be disabled or removed

10.10.9 BYOD devices should have the operating system firewall switched on and enabled.

Working From Home / Remote Working

10.11 While working away from the office, special considerations must be made regarding your working environment and the people around you to ensure data security.

10.12 Personal or sensitive data must only be saved or transferred to College-approved systems.

10.13 All electronic storage devices containing internal or confidential classified information must be encrypted by the IT Department before being taken off-site.

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

10.15 IT resources must not be connected to unsecured, public, or unknown Wi-Fi networks.

- Further guidance on the use of public WIFI is available from the NCSC website: https://www.ncsc.gov.uk/collection/end-user-device-security?curPage=/collection/end-user-device-security/eud-overview/common-questions#wifi

10.16 Remote access to the College Domain is only available via equipment purchased by the IT Department.

10.17 VPN access to College systems is not available for personal devices.

10.18 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 the office.

- College mobile phones will not be issued specifically for MFA purposes

Mobile Phone Personal Hotspot (Tethering) Usage

10.19 Mobile phones can be configured to connect to your laptop to access College services where a secure Wi-Fi signal is not available. This is sometimes referred to as tethering.

10.20 The following usage guidelines must be closely observed when using a personal hotspot:

10.20.1 The personal hotspot must only be used when a secure Wi-Fi network is not available.

10.20.2 You will be responsible for any data charges associated with connecting a College-issued laptop to your personal mobile phone, unless you have written approval from the budget holder before use.

10.20.3 The personal hotspot on a College-issued mobile must only be connected to your College-issued laptop and used for Weston College work purposes. It should not be used for streaming media or transferring large files.

10.20.4 The personal hotspot on a College-issued mobile must not be used for personal use and must not be connected to personal devices.

10.20.5 All personal hotspots must be configured using a strong password based on the #ThreeRandomWords guidance from the NCSC.

10.20.6 The personal hotspot password must not be shared with anyone.

10.20.7 Weston College reserves the right to invoice staff for data usage where this policy has not been followed.

Loan of Staff Equipment

10.21 IT resources may be available for users to take off-site.

10.22 A loan equipment form must be signed, agreeing to the terms and conditions of the loan, before any IT resources are taken off-site.

10.23 All IT resources must be collected in person; devices will not be issued to anyone else.

10.24 Loaned IT resources must only be used by the user for whom they have been configured and who has signed the Loan Equipment Form.

10.25 Loaned IT resources must not be used by:

10.25.1 Any member of staff other than the person who has signed the Loan Equipment Form

10.25.2 Any learner

10.25.3 Any friends or family members

10.25.4 Anyone other than the User who has signed the Loan Equipment Form

10.26 The geographic location of College-owned equipment may be tracked.

10.27 Users must apply any security updates for loaned IT resources within five working days of being notified that an update is available.

10.28 Any loaned IT resources not updated within five working days will be disabled, and the loaned IT resources must be returned to the IT Department within the next five working days for checking and reactivation.

10.29 The IT Department reserves the right to request the return of loaned IT resources at any time.

10.30 Loaned IT resources must be returned to the IT Department within five working days of a return being requested.

10.31 Loaned IT resources are vulnerable to theft and must never be left within view of the public, including within vehicles.

10.32 Users may be invoiced for the repair or replacement of any lost or damaged loaned IT resources. Therefore, it is recommended that users check that loaned IT resources are covered by home and car insurance policies in the event of theft.

10.33 Users may be invoiced for any equipment that has not been returned to the IT Helpdesk within five days of it being requested.

10.34 IT resources must never be used while driving.

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

10.36 College-issued mobile devices are pre-configured with drive encryption to help protect against data loss from theft.

10.37 Users are reminded that drive encryption is only effective if the “threat actor” cannot obtain or guess the user's password.

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

10.39 If an IT device has been lost or stolen, it must be reported to the IT Helpdesk (01934 411425) immediately.

11 IT RESOURCES

Requesting IT Resources

11.1 Additional IT resources are generally requested within the annual strategic planning process.

11.2 All electronic storage devices intended to store internal or confidential classified information must be purchased via the IT Department.

11.3 Staff may request IT resources mid-year by completing the Inventory Request Form on the Finance SharePoint site.

11.4 All IT resources must be purchased in accordance with the Financial Regulations and Procurement Strategy.

11.5 IT resources must be returned to the IT Helpdesk before they can be reallocated to other members of staff.

Disposal of IT Resources

11.6 All IT resources must be disposed of through the IT Department, utilising a registered IT disposal company that holds ISO 27001 data security certification and complies with the Waste Electrical and Electronic Equipment (WEEE) Directive.

11.7 A secure disposal certificate must be obtained for the disposal of all electronic storage devices that have contained internal or confidential classified information.

11.8 The sale or donation of any College IT resources is prohibited without the written approval of the Head of IT.

11.9 Upon request or termination of employment, all IT resources must be returned to the IT Helpdesk.

12 IT SUPPORT AND INCIDENT MANAGEMENT

12.1 All issues and information security incidents related to IT resources or systems must be reported to the IT Helpdesk.

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

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

12.4 All criminal related incidents will be reported to Action Fraud for legal investigation.

13 RESPONSIBILITIES

Compliance, Monitoring and Review

13.1 Weston College Governing Body is responsible for:

- Approval of this policy

13.2 Weston College Group Executive Team are responsible for:

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

13.3 Director of IT is responsible for:

- Ensure this policy meets legal & regulatory requirements
- Ensure a robust, risk-based approach to cybersecurity
- Ensure a flexible approach to IT delivery
- Investigate any breach of policy.
- Report any IT related concerns to Chief Operating Officer

13.4 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 the IT Helpdesk for investigation

Reporting

13.5 No additional reporting is required.

Records management

13.6 Staff must maintain all records relevant to administering this policy using the ISMS Control of Information Assets Procedure (WCGIT-1214890995-8).

14 DEFINITIONS

Terms and definitions

Bring Your Own Network (BYON): The practice of using personal network devices, such as mobile hotspots, to access the internet or organisational resources.

BYOD: Bring Your Own Device, A term used for using personally owned devices to access Weston College systems and Information Assets.

Clear Desk & Clear Screen Policy: A policy ensuring that sensitive information is securely stored and screens are locked when not in use, maintaining a tidy workspace and protecting confidential data.

Counter Terrorism Internet Referral Unit (CTIRU): A UK police unit responsible for identifying and removing online content that promotes terrorism or extremism.

Data Sharing Agreement (DSA): A formal agreement between parties outlining the terms and conditions for sharing data, ensuring compliance with data protection laws and safeguarding sensitive information.

Eduroam: A global Wi-Fi service that provides secure and easy internet access to students, researchers, and staff at participating institutions.

Information Assets: Any form of information, document or data which has value to the Weston College Group

Information Security Incident: An event that has caused or could lead to compromising the Confidentiality, Integrity or Accessibility (CIA) of an Information Asset

Information Security Management System (ISMS): Collection of policies and procedures which define how the College manages information Assets

Information Security Steering Group (ISSG): Collection of policies and procedures which define how the College manages information Assets

Information Security: Protecting against the unauthorised use of Information Assets

Information Users: Any members of staff, learner, associate, partner and stakeholder who interact with Weston College Group Information Assets

Internet Watch Foundation (IWF): A UK-based organisation that works to eliminate online child sexual abuse content and other harmful material from the internet.

IT Helpdesk – Support desk for IT services contact 01934 411425 | it.helpdesk@weston.ac.uk

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

JANET Network: A high-speed network for the UK research and education community, providing internet access and other services to universities, colleges, and research institutions.

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

National Cyber Security Centre (NCSC): A UK government organisation that provides advice and support for the public and private sectors on how to avoid computer security threats.

Personally Identifiable Information (PII) – The ICO's definition of information can be used to identify an individual.

Prevent: A UK government strategy aimed at preventing individuals from becoming involved in terrorism or supporting extremist causes.

Single Sign-On (SSO): An authentication process that allows a user to access multiple applications with one set of login credentials, reducing the number of passwords users need to remember.

Software: The term software is used to refer to any executable code and all licencing type both paid for and free. This includes but not limited to installable applications(apps), portable applications(apps), system software, middleware, drivers, databases, utilities, plugins, interpreters, scripts, libraries, shareware, opensource, proprietary.

Three Random Words: A password creation technique recommended by the National Cyber Security Centre (NCSC) that involves using three random words to create a strong, memorable password.

User Account: Username & Password used to login to the Weston College Group network

Users: Enrolled students, members of staff and associates

Virtual Private Network (VPN): A secure network connection over the internet that encrypts data and provides privacy and anonymity for users accessing the network remotely.

15 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

- IT Security Policy (WCGIT-535199308-2)
- Data Sharing Agreement (WC_PRN_305)
- Information Security Policy (WCGIT-1214890995-12

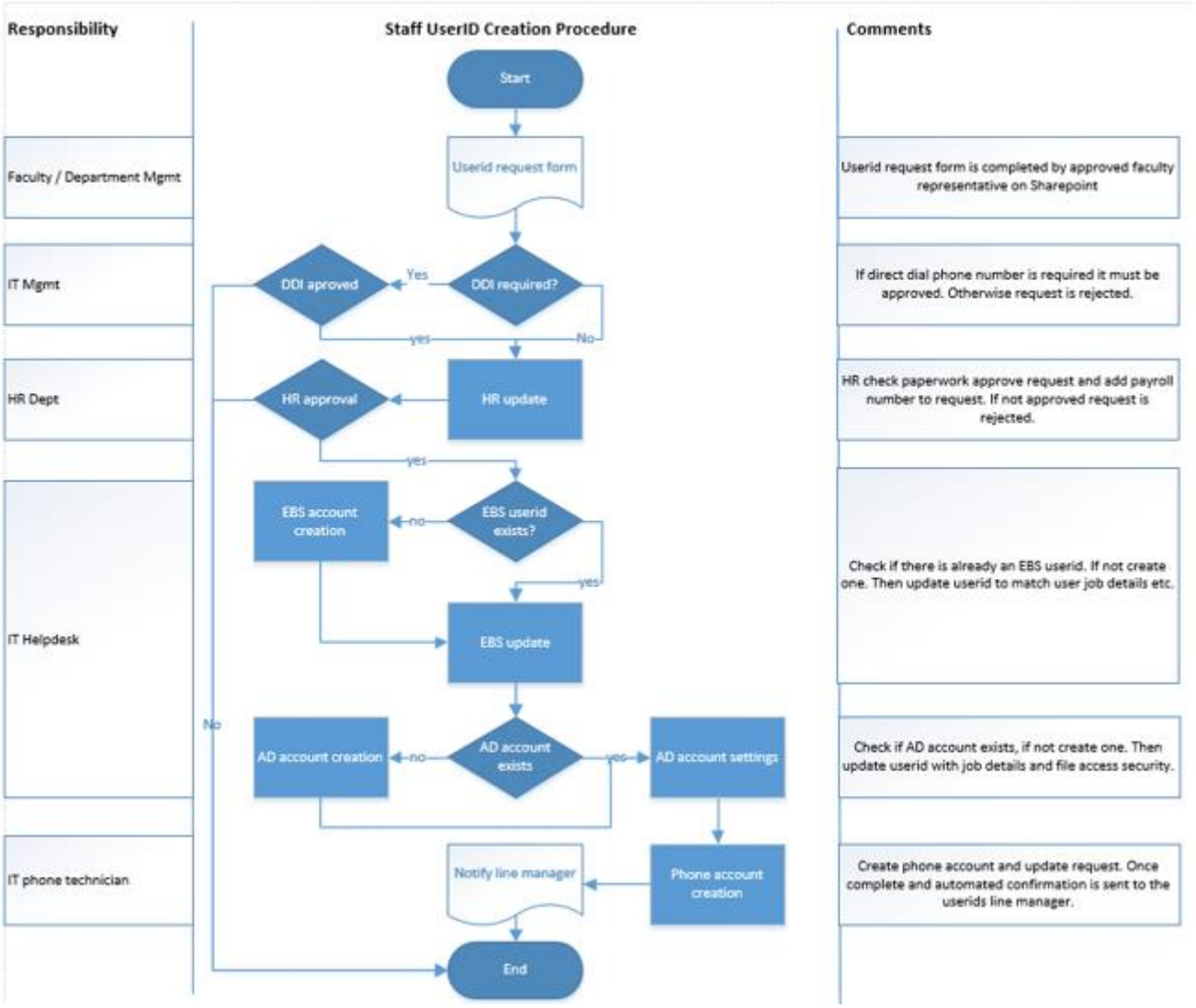
3rd Party Policies, Procedures, Terms & Conditions

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

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

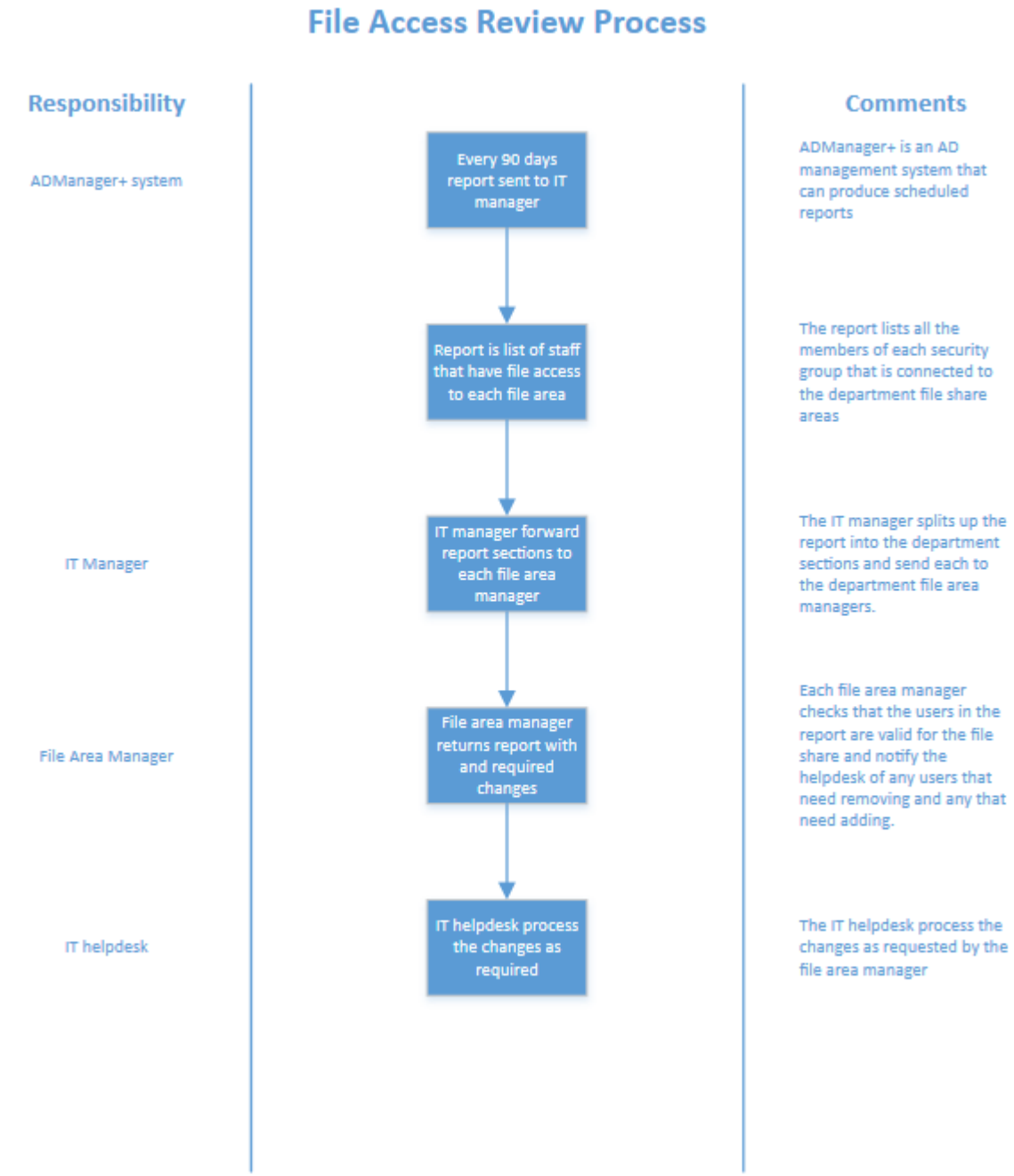
16 APPENDIX A

Staff Account Creation Process



17 APPENDIX B

File Access Review Process



18 APPENDIX C

Complex Password Rules

The following rules apply to all user account passwords:

- a minimum of 8 characters long
- must not contain the User's: First, Middle or Last Names
- must not have been used before
- must be changed every 60 days.
- must contain characters from three of the following five categories:
  1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
  3. Base 10 digits (0 through 9)
  4. Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
  5. Any Unicode character that is categorised as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

19 APPENDIX D

19.1 Password Recommendations

Your password is a critical component to the cyber security of the network, this document uses recommendations from the National Cyber Security Centre who are part of GCHQ.

Three Random Words

Three random words or #thinkrandom - NCSC.GOV.UK

Using 3x random words within your password makes you password, long, complex but still easy to remember (after about a week of using it).

The words must be random and not of your personal choosing or linked to you in any way.

If you need inspiration and to keep it random use a website to suggest your words. Examples of random word generating websites include

- www.randomwordgenerator.com
- www.wordcounter.net
- www.randomlists.com

Complexity Rules

Once you have your 3x words, follow these steps to ensure you meet the complexity rules

1. Capitalise some or all of your words
2. Add a random number between the first and second word
3. Add a random symbol between the second and third word

The Final Password

Your final password will have the following format:

<word1><number><word2><symbol><word3>

An example of a password generated using this technique would be:

Alive2Chew!March

Multi Factor Authentication

Where Multi Factor Authentication (MFA) or 2 Factor Authentication (2FA) options are available they should always be enabled and used.