Weston College Group

IT ACCEPTABLE USE POLICY

IT ACCEPTABLE USE POLICY

CONTENTS

Change Control

Version:	3.0
Date approved by CLB:	January 2022
Date approved by Corporation:	N/a – Authority for approval of operational policy deligaed to CLB
Name and title of policy holder:	Matt Beaver, Head of IT
Date issued:	January 2022
Review date:	January 2023

Version	**Type – New/Replacement/Review**	**Date**	**History**
1.0	Replacement	Dec 2019	New document template Reviewed & approved by CLB & Governors
2.0	Review	Dec 2020	Reviewed & approved by CLB & Governors
3.0	Review	Jan 2022	Updated with Sexual Abuse in Colleges focus. Updated BYOD following COVID Lockdown Updated BYOD to align with Cyber Essentials Requirements Updated to align with ISO 27001 requirements and wording

This policy applies to Weston College Group and all wholly-owned subsidiary companies of the Weston College Corporation which include PEF, Forward Futures, SOMAX, Releasing New Potential, Inspirational Events and Investments

IT ACCEPTABLE USE POLICY

1 PURPOSE

1.1 The Weston College Group offers a wide range of **IT Resources** which are free to use for their **Users**.

1.2 To use the Weston College Group **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.

2 SCOPE

2.1 This policy covers:

- All companies and subsidiaries of the Weston College Group
- Anyone who uses any Weston College Group **IT resources** or services (including online services)

Offender Learning

2.2 Offender Learning is referred to within this policy but **Users** of Offender Learning Networks within prisons where the College delivers the Prison Education Network (PEF) must comply with the HMPPS/MOJ approved PEF IT Security Procedure and any other local HMP or HMPPS/MOJ policies and procedures applicable.

3 ACCESS CONTROL POLICY *Incorporating ISO 27001 Annex A.9.*

3.1 Access to The Weston College Group **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 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 request **User Accounts** for staff via the New User Request Form on SharePoint.
- Appendix A shows the staff account creation process

3.7 Tutor Accounts (t. Accounts)

- Tutor Accounts will be automatically created when new Staff Accounts are created

- Appendix A shows the staff account creation process

3.8 Learner Accounts

- Learners' **User Accounts** will be automatically created 24 hours after being enrolled on an active course

User Account Removal

3.9 Staff Accounts

- Staff **User Accounts** will be automatically deactivated on the end date of their contract.

3.10 Tutor Accounts (t. Accounts)

- Tutor Accounts will be deactivated at the same time as staff accounts

3.11 Learners Accounts

- Learners' **User Accounts** can be disabled at any time by a faculty manager contacting the **IT Helpdesk.** All non-active Learners **User Accounts** will be automatically disabled on the completion of their course.

Guest / Generic Accounts

3.12 Weston College does not provide Guest / Generic **User accounts**.

3.13 All **user accounts** must be associated with an individual, except where approved by the Head of IT

3.14 Guest WIFI is available for visitors please refer to the **BYOD** section for more information

Administration Accounts

3.15 Administration permissions to the domain and local computers are limited to members of the IT Department.

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

3.17 The number of **User Accounts** assigned special access or administration permissions will be typically limited to 5 **User Accounts** per system.

3.18 Special access & administration group membership will be monitored and reviewed annually.

Access Control

3.19 Access to systems and resources are restricted by permissions. To request additional access please contact the **IT Helpdesk** for guidance.

3.20 Access to **IT Resources** may be removed by system owners, the HR department or a member of the Corporate Leadership Board by contacting the **IT Helpdesk** (it.helpdesk@weston.ac.uk).

3.21 All requests for permission changes must be requested by email, an **IT helpdesk** call will be raised for all permission changes as an audit record.

3.22 The IT Department regularly monitor file access permissions following the process shown in Appendix B

Passwords & Authentication

3.23 Weston 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 written or saved on electronic devices.
- Passwords may be changed at any time. Please contact the **IT Helpdesk** for further assistance or advice on passwords.
- 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 Account**.
- **User Accounts** will automatically be locked out after 5 incorrect password attempts.

3.24 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

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

Reduce Reliance on passwords

3.26 Weston College use single sign-on (SSO) where available to reduce the number of passwords **users** are required to remember & enter

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

3.27 **Multi-Factor Authentication (MFA)** is used to improve the security of Weston College **user accounts**

3.28 **Users** will be required to register a personal device to confirm their identity

3.29 **Users** will occasionally be asked to enter a code sent to their registered device when logging in from outside the Weston College network

Password Managers

3.30 A password manager is an app within your web browser that stores your passwords securely, so you don’t need to remember them all, making it easier to log on. They can also create random, unique passwords for you when you need to create a new password (or change an existing one).

3.31 Weston College supports the use of LastPass password management software.

3.32 LastPass Plugins are available for **Users** to download and install for the Edge and Chrome web browsers

Offender Learning

3.33 All offender learning **User Accounts** must be created in accordance with the PEF Account Creation Procedure.

4 DATA SECURITY

Clear Desk & Clear Screen Policy
Incorporating ISO 27001 Annex A.11.2.9

4.1 To ensure data security, the College has a clear screen & desk policy, this means:

- Computers must be locked EVERY TIME you leave your 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 you leave your desk.
- 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.

4.2 **Information Assets** containing **Personally Identifiable Information** must never be taken, copied or downloaded onto personal computers or systems outside of the College's network. Please refer to the Information Security Policy for more details.

Personal Data, Accounts, Removal Media & Services

4.3 **Personally Identifiable Information** or information classified as Internal or Confidential **Information Assets** must never be sent or saved to personal accounts, devices or removable media.

This includes:

- Personal email accounts
- Personal cloud 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…

4.4 Emails, **Information Assets** may be accessed via mobile apps and web browsers, but **Personally, Identifiable Information** & confidential **Information Assets** must never be saved to personal devices. If in doubt, please contact it.helpdesk@weston.ac.uk for advice.

4.5 **Personally, Identifiable Information** & confidential **Information Assets** may only be shared with external companies, contractors or individuals where a data-sharing agreement and/or Non-Disclosure Agreement (NDA) has been signed by both parties.

4.6 **Personally, Identifiable Information** & confidential **Information Assets** must only be sent to permitted external companies, contractors or individuals using a secure encrypted method of transfer. For advice please contact it.helpdesk@weston.ac.uk.

4.7 All **Information Assets** must be saved to approved College servers or services.

4.8 Backups of **Personally Identifiable Information** & confidential **Information Assets** information by Learners and Staff are not permitted.

4.9 All **IT Resources** must be configured and connected to a Weston College Group domain by the IT Department.

4.10 **Offender Learning –** The use of USB storage devices within offender learning environments are strictly controlled. Please refer to the HMPPS/MOJ approved PEF IT Security Procedure for more information

Non-Work-Related Data and Documents

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

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

4.13 Weston College Group 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.

4.14 Weston College Group reserves the right to delete or prevent access to any private or personal non-work-related stored on College servers or 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 MONITORING & LOGGING

5.1 Weston College monitors and logs data relating to all **IT Resources, Information Assets** and College systems.

5.2 Monitoring and logging include:

- Login / Logout
- File Activity
- Internet Activity
- Communication
- Location Tracking of equipment
- Screen capture

5.3 By logging into **IT Resources** you agree that data identifying you as an individual can be securely stored and used by the Weston College Group to investigate breaches of this policy.

5.4 Where officially requested, this data will be sent to local authorities for criminal investigations.

6 PHYSICAL SECURITY

Vandalism

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

6.2 Any costs incurred repairing or replacing vandalised equipment will be charged to anyone caught vandalising **IT Resources**.

6.3 To minimise the risk of accidental damage to **IT Resources**, Food & Drink is not permitted in any Library Plus or computer suites.

6.4 **Users** are not permitted to unplug or move any non-mobile **IT Resources**.

7 SOFTWARE

7.1 **Users** are not permitted to install software on any **IT Resources** this includes running portable applications.

7.2 The installation of software applications can be requested via the **IT Helpdesk**.

7.3 The use of cloud-based software applications which store personal information of learners or staff must be approved by the IT Department or the Business Information & Intelligence Group (BIIG)

7.4 **Offender Learning -** All Software and media files used on the Offender Learning networks must be compliant with HMPPS Policies. (PEF IT Security Procedure 6.0)

8 MALWARE

8.1 The Weston College Group use several layers of security systems to protect data and **IT Resources** from viruses and malware.

8.2 **Users** must report to the **IT Helpdesk** if a computer virus has been identified.

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

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

9 INTERNET ACCESS

9.1 Weston College internet access is provided via the JANET National network. While using the internet all **Users** must agree to the JANET Acceptable Use Policy.

9.2 Weston College E-Safety & Social Media Policy details acceptable online behaviours and electronic communication and the additional responsibilities which you must accept before accessing Social Media sites.

9.3 Weston College uses a web filtering solution to block access websites that 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.

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

9.5 Misuse of Weston College Group Internet Access or any attempt to circumvent security systems including web filtering may result in disciplinary and/or legal action.

Safeguarding and Prevent

9.6 The following harmful & unacceptable activities are actively monitored and logged as part of the College's responsibility towards multi-agency Safeguarding, Prevent & Sexual abuse in Colleges agendas.

- The information which may lead to potential terrorism or extremist activity
  - Internet activity including sites categorised as:
    - Intolerance
    - Personal Weapons
    - Terrorism
    - Violence

- The information which may identify harmful sexual behaviour which may be a potential risk to young people or vulnerable adults
    - Internet activity including sites categorised as:
        - Adult Entertainers
        - Adult Sites
        - Child Abuse
        - Pornography
        - Restricted to Adults

9.7 Logs and information relating to Safeguarding, Prevent or indicate behaviours relating to 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

9.8 Downloading or streaming copyrighted material that you are not licenced to view/access may result in disciplinary and/or legal action.

9.9 The use of Peer to Peer software including BitTorrent is not permitted to run while connected to any Weston College Group networks.

9.10 Access to the Dark Web or Tor Networks is not permitted while connected to any Weston College Group networks.

9.11 **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

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

9.13 HE **users** (Staff and Learners) must not access material that is illegal and/or without proper licensing doing so may result in disciplinary and/or legal action.

9.14 HE **users** (Staff and Learners) must only access web resources where it is connected with the academic requirements of the HE programme and is for educational purposes only.

9.15 HE **users** (Staff and Learners) must exercise considerable care and responsibility in sites that are accessed. For safeguarding purposes, if children or vulnerable adults are present, the FE IT Policy applies.

Internet Access for Offender Learning

9.16 Internet Access is forbidden on the Weston College Offender Learning networks.

9.17 The student shared drives are regularly monitored for suspicious activity. If detected this is reported to the **IT Helpdesk** immediately. (PEF Account Creation Procedure 5.0)

9.18 If access to the internet is found to be available on the educational network, this should be reported to the **IT Helpdesk** immediately.

10 MOBILE DEVICE POLICY

Incorporating ISO 27001 Annex A.6

Bring Your Own Device (BYOD)

10.1 **Users** may connect their own devices to the College Guest WIFI service using the eduroam service and their **User Account** details. **Users** must agree to the **eduroam UK policy** to use this service.

10.2 **Users'** Own Devices may be connected by WIFI only, connecting via Ethernet cable is not permitted.

10.3 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.

10.4 IT support services are unable to support **Users'** own devices, including the recovery of data. If experiencing issues, please use the **IT Resources** supplied by The Weston College Group.

10.5 IT support will not install any drivers or software on **IT Resources** to support personal devices

10.6 Personal Hotspots or Bring Your Own Network (BYON) are not permitted.

10.7 Use of anonymizing, VPN or proxy software is not permitted on any Weston College Group networks.

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

10.9 Before connecting a **BYOD** device to a Weston College system or data you must ensure your device meets the following Cyber Essentials Certification requirements:

10.9.1 **BYOD** devices must be currently supported by the manufacturer and have the latest system/firmware updates installed

10.9.2 **BYOD** devices are running a currently supported operating system that has the latest updates installed.

10.9.3 **BYOD** devices only have currently supported applications with the latest updates installed

10.9.4 **BYOD** devices must be running up 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

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

10.9.6 **BYOD** devices must 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

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

10.9.8 **BYOD** devices that are shared with family and friends and used to access Weston College systems must 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

10.9.9 **BYOD** devices must have the operating system firewall switched on and enabled.

10.10 **Offender Learning -** Personal IT devices are not permitted to be connected or used in Offender Learning classrooms.

Working From Home

10.11 While working away from the office, special considerations must be made to 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 **Users** must assess their environment and position of screens so they cannot be viewed by others.

10.14 **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: https://www.ncsc.gov.uk/collection/end-user-device-security?curPage=/collection/end-user-device-security/eud-overview/common-questions#wifi

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

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

10.17 **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 specifically for MFA purposes

Loan Equipment

10.18 **IT Resources** may be available for **Users** to take off-site.

10.19 A Loan Equipment Form must be signed agreeing to the terms and conditions of the loan before any loaned **IT Resources** are taken off-site.

10.20 All **IT Resources** must be collected in person, devices will not be issued to anyone else.

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

10.22 Loaned **IT Resources** must only be used by the **user** for who it has been configured for and who has signed the Loan Equipment Form.

10.23 Loaned **IT Resources** must not be used by:

- Any member of staff other than who has signed the Loan Equipment Form
- Any learner
- Any friends or family member
- Anyone other than the **User** who has signed the Loan Equipment Form

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

10.25 **Users** must apply any security updates for loaned **IT Resources** within 5 working days of being notified an update is available.

10.26 Any loaned **IT Resources** not updated within 5 working days will be disabled and the loaned **IT Resources** must be returned to the IT Department with the next 5 working days.

10.27 The IT Department reserve the right to request the return of loaned **IT Resources** at any time.

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

10.29 Loaned **IT Resources** are vulnerable to theft and must never be left within view of the public including within vehicles. Kensington Locks are available via the **IT Helpdesk** if required.

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

10.31 **Users** may be invoiced for the repair or replacement of any lost or damaged loaned **IT Resources**.

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

10.33 **IT Resources** must never be used while driving.

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

10.35 The college issued mobile devices are pre-configured with drive encryption to help protect loss of data from theft.

- **Users** are 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.

10.36 If a mobile 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 Staff may request **IT Resources** mid-year by completing the Inventory Request Form on the Finance SharePoint site.

11.3 All **IT Resources** must be purchased in accordance with the Financial Regulations and Procurement Strategy.

11.4 **IT Resources** must be returned to the **IT Helpdesk** before they can be reallocated to other members of staff

Disposal of IT Resources

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

11.6 The sale or donation of any Weston College Group I**T Resources** is not permitted without the written approval of the Head of IT.

11.7 Upon request or leaving employment all **IT Resources** must be returned to the **IT Helpdesk.**

12 IT SUPPORT

12.1 All issues / **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 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.

12.5 **Offender Learning -** Offender Learning **Users** should follow the PEF IT Support Procedure.

13 RESPONSIBILITIES

Compliance, Monitoring and Review

13.1 Weston College Governing Body is responsible for:

- Overseeing approval of this policy

13.2 Weston College Group Corporate Leadership Board (CLB) is responsible for:

- Approval of policy on behalf of the governing body
- Ensure this policy reinforces the strategic objectives of the College

13.3 Head 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 the relevant CLB Lead

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

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

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

Information Security: Protecting against the unauthorized use of Information Assets
Information Users: Any members of staff, learner, associate, partner and stakeholder who interact with Weston College Group Information Assets

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

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...

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

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 Weston College Group network

Users: Enrolled students, members of staff and associates

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

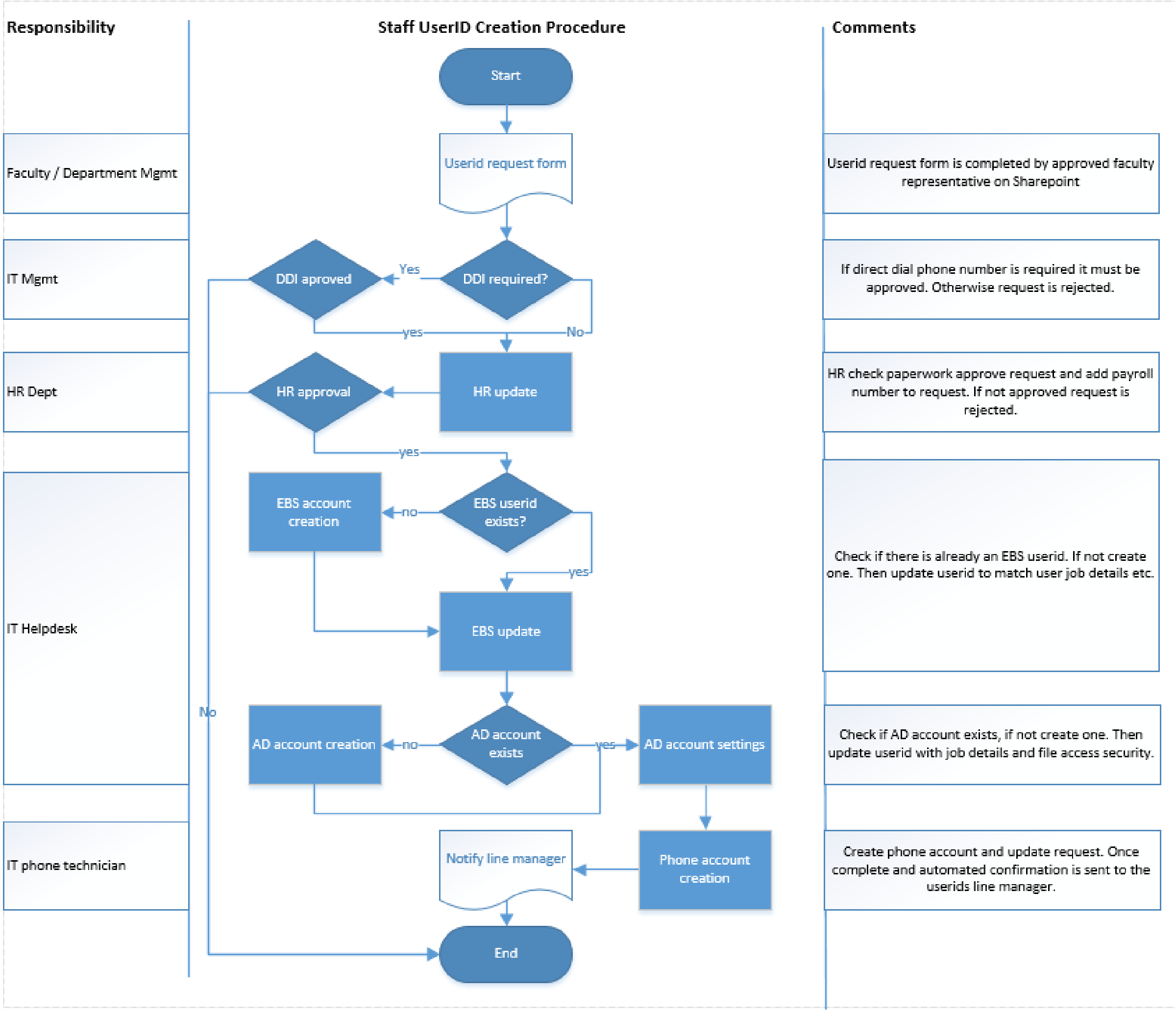
Offender Learning

Users who are Offender Learners or delivering Offender Learning contracts must also comply with the following policies:

- Her Majesty's Prisons and Probation Service (HMPPS) IT Policies
- Local Prison IT Policies

16 APPENDIX A

Staff Account Creation Process

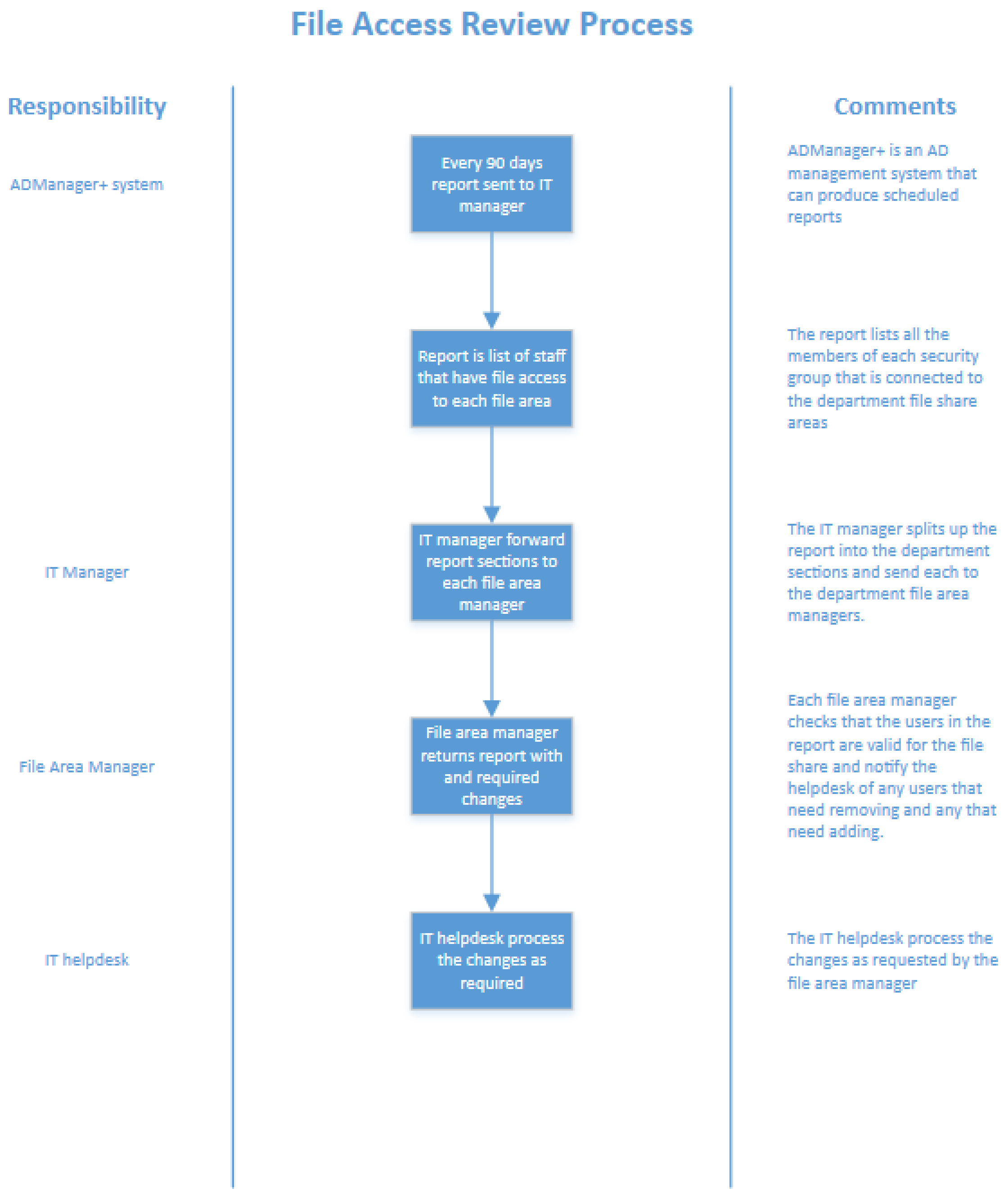


Responsibility	Comments
Faculty / Department Mgmt	Userid request form is completed by approved faculty representative on Sharepoint
IT Mgmt	If direct dial phone number is required it must be approved. Otherwise request is rejected.
HR Dept	HR check paperwork approve request and add payroll number to request. If not approved request is rejected.
IT Helpdesk	Check if there is already an EBS userid. If not create one. Then update userid to match user job details etc. Check if AD account exists, if not create one. Then update userid with job details and file access security.
IT phone technician	Create phone account and update request. Once complete and automated confirmation is sent to the userids line manager.

Once PRINTED, this is an UNCONTROLLED DOCUMENT.

17 APPENDIX B

File Access Review Process


File Access Review Process
Responsibility
Comments
ADManager+ system
Every 90 days report sent to IT manager
Report is list of staff that have file access to each file area
IT Manager
IT manager forward report sections to each file area manager
File Area Manager
File area manager returns report with and required changes
IT helpdesk
IT helpdesk process the changes as required

ADManager+ is an AD management system that can produce scheduled reports

The report lists all the members of each security group that is connected to the department file share areas

The IT manager splits up the report into the department sections and send each to the department file area managers.

Each file area manager checks that the users in the report are valid for the file share and notify the helpdesk of any users that need removing and any that need adding.

The IT helpdesk process the changes as requested by the file area manager

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 categorized 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.