Weston College Group

IT ACCEPTABLE USE POLICY

IT ACCEPTABLE USE POLICY

CONTENTS

IT ACCEPTABLE USE POLICY

Change Control

Version:	1.1
Date approved by CLB:	4th December 2020
Date approved by Corporation:	15th December 2020 
Name of policy holder:	Matt Beaver
Date issued:	15/12/2020
Review date:	December 2021

Version	Type – New/Replacement/Review	Date	History
1.1	Review	December 2021	

This policy applies to Weston College Group and all wholly-owned subsidiary companies of the Weston College Corporation which include OLASS, Forward Futures, WoEI, 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 POLICY STATEMENT

User Accounts & Access Control

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

Offender Learning

3.23 All offender learning User Accounts must be created in accordance with the OLASS Account Creation Procedure.

Passwords & Authentication

3.24 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.

3.25 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

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

Reduce Reliance on passwords

3.27 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)

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

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

3.30 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

3.31 A password manager is an app on 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).

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

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

Data Security

3.34 To ensure the 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.

3.35 Documents and data containing personal data 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.

Monitoring and Logging

3.36 The Weston College Group monitor and log data for all IT Resources.

3.37 Monitoring and logging include:

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

3.38 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.

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

Safeguarding and Prevent

3.40 The following activity is actively monitored and logged as part of the College's responsibility towards multi-agency safeguarding and PREVENT 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 lead to 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

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

3.42 **Offender Learning -** Student shared drives are regularly monitored for suspicious activity. If detected this is reported to the IT Helpdesk immediately. (OLASS Account Creation Procedure 5.0)

Vandalism

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

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

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

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

Software

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

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

3.49 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)

3.50 **Offender Learning -** All Software and media files used on the Offender Learning networks must be compliant to NOMs Policies. (OLASS IT Security Procedure 6.0)

Viruses & Malware

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

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

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

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

Internet Access

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

3.56 The Weston College Group 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.

3.57 The College uses a web filtering solution to block access 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.

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

3.59 Downloading or streaming of copyrighted material which you are not licenced to view/access will result in disciplinary or legal action.

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

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

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

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

3.64 **Offender Learning -** Internet Access is forbidden on the Weston College Offender Learning networks.

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

Internet Access for Higher Education

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

3.67 HE users (Staff and Learners) must not deliberately or knowingly seek to access material that is illegal and/or without proper licensing.

3.68 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.

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

Bring Your Own Device (BYOD) / Personal Devices

3.70 **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.

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

3.72 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.

3.73 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.

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

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

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

3.77 BYOD devices must have the latest operating system and application updates installed before connecting at any Weston College systems or data

3.78 Vintage or obsolete devices which no longer receives updates. Must not be used to access Weston College systems or data

3.79 BYOD devices must be running an un-modifed version of the manufactures supported operating system, Jailbroken devices must not be used to access Weston College systems or data.

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

3.81 BYOD devices must be configure with separate login profiles so Weston College systems and data are kept away from

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

Working From Home

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

3.84 Data containing personal or sensitive information must not be taken out on the College unless encrypted.

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

3.86 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

3.87 Remote access to the College Domain is only available via equipment purchase by the IT Department.

3.88 VPN access is not available for personal devices.

3.89 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

Loan Equipment

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

3.91 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.

3.92 All devices must be collected in person, devices will not be issued to anyone else.

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

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

3.95 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

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

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

3.98 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.

3.99 The IT Department reserve the right request the return of loaned IT Resources at any time.

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

3.101 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.

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

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

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

3.105 IT Resources must never be used while driving.

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

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

- 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 most not be kept with the device.

3.108 If a mobile device has been lost or stolen it must be reported to the IT Helpdesk (01934 411425) immediately.

Data Security, Removable Media & Backups

3.109 Personal & Confidential 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…

3.110 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 it.helpdesk@weston.ac.uk for advice.

3.111 Personal & Confidential information 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.

3.112 Personal & Confidential information 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.

3.113 All data must be saved to approved College servers or services.

3.114 Backups of Personal & Confidential information by Users is not permitted.

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

3.116 **Offender Learning –** 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

3.117 Only data relating to the Weston College Groups' business are to be saved on College servers, systems or databases.

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

3.119 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.

3.120 Weston College Group reserves the rights 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.

3.121 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

3.122 Additional IT Resources are generally requested within the annual strategic planning process.

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

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

3.125 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.

3.126 The sale or donation of any Weston College Group IT Resources is not permitted.

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

3.128 If IT resources need to be reallocated, they must be returned to the IT Helpdesk first for reallocation

IT Support

3.129 All issues/incidents with IT equipment or systems must be reported to the IT Helpdesk.

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

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

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

3.133 **Offender Learning -** Offender Learning Users should follow the OLASS IT Support Procedure.

4 RESPONSIBILITIES

Compliance, Monitoring and Review

4.1 Weston College Governing Body is responsible for:

- Approval of this policy

4.2 Weston College Group Corporate Leadership Board (CLB) 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:

- 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

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 the IT Helpdesk for investigation

Reporting

4.5 No additional reporting is required.

Records management

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

5 DEFINITIONS

Terms and definitions

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

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

Information Security Incident: An event which 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 unauthorized use of Information Assets
Information Users: Any members of staff, learner, associate, partner and stakeholder who interact with Weston College Group Information Assets

IT Helpdesk – Support desk for IT services contact 01934 411425 | it.helpdesk@weston.ac.uk
IT Resources – include Computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, equipment, software, services, 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 Weston College Group network

Users: Enrolled students, members of staff and associates

6 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

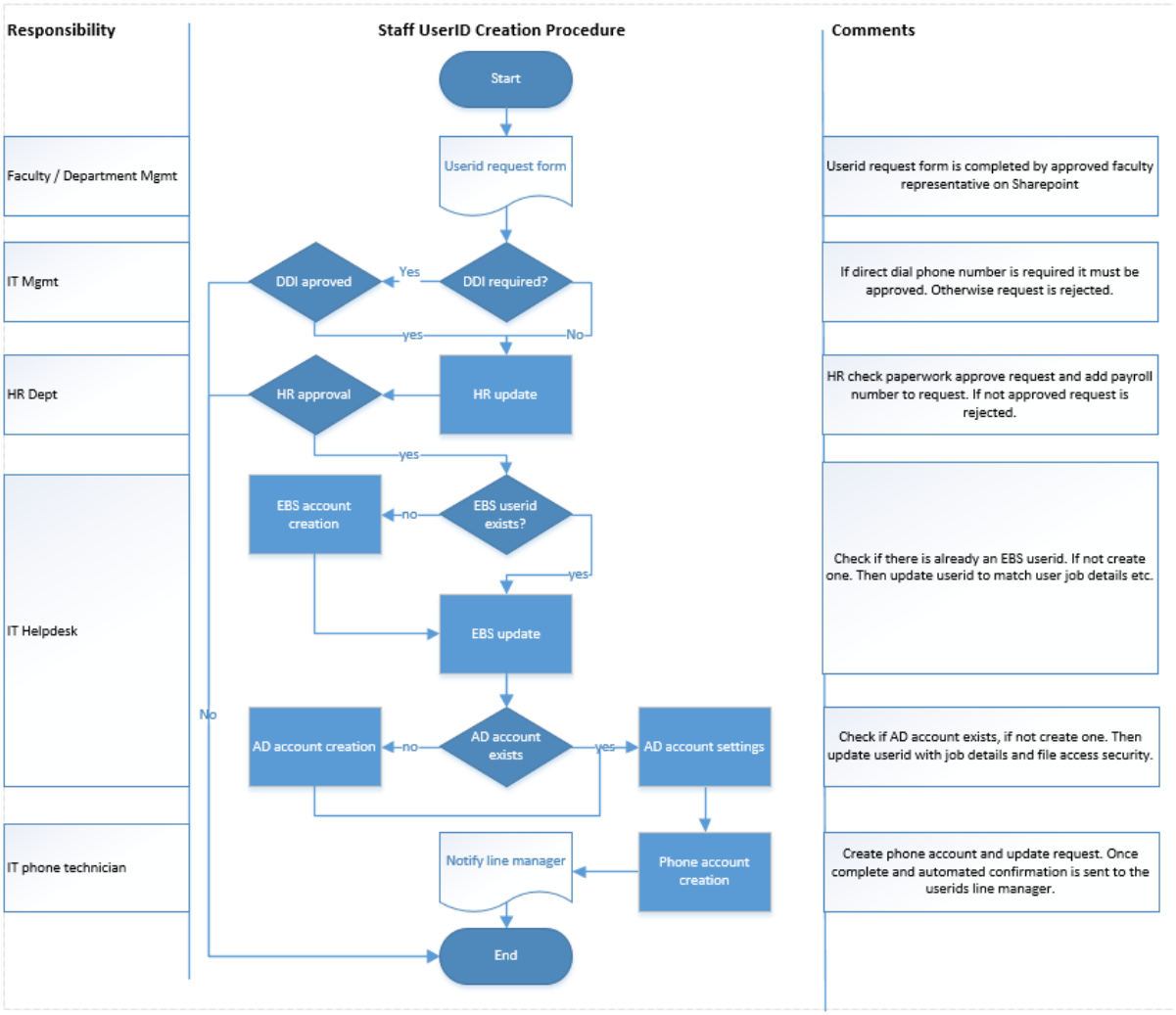
Offender Learning

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

- National Offenders Management Service (NOMS) IT Policies
- Local Prison IT Policies
- Immigration Retention Centre (IRC) IT Policies

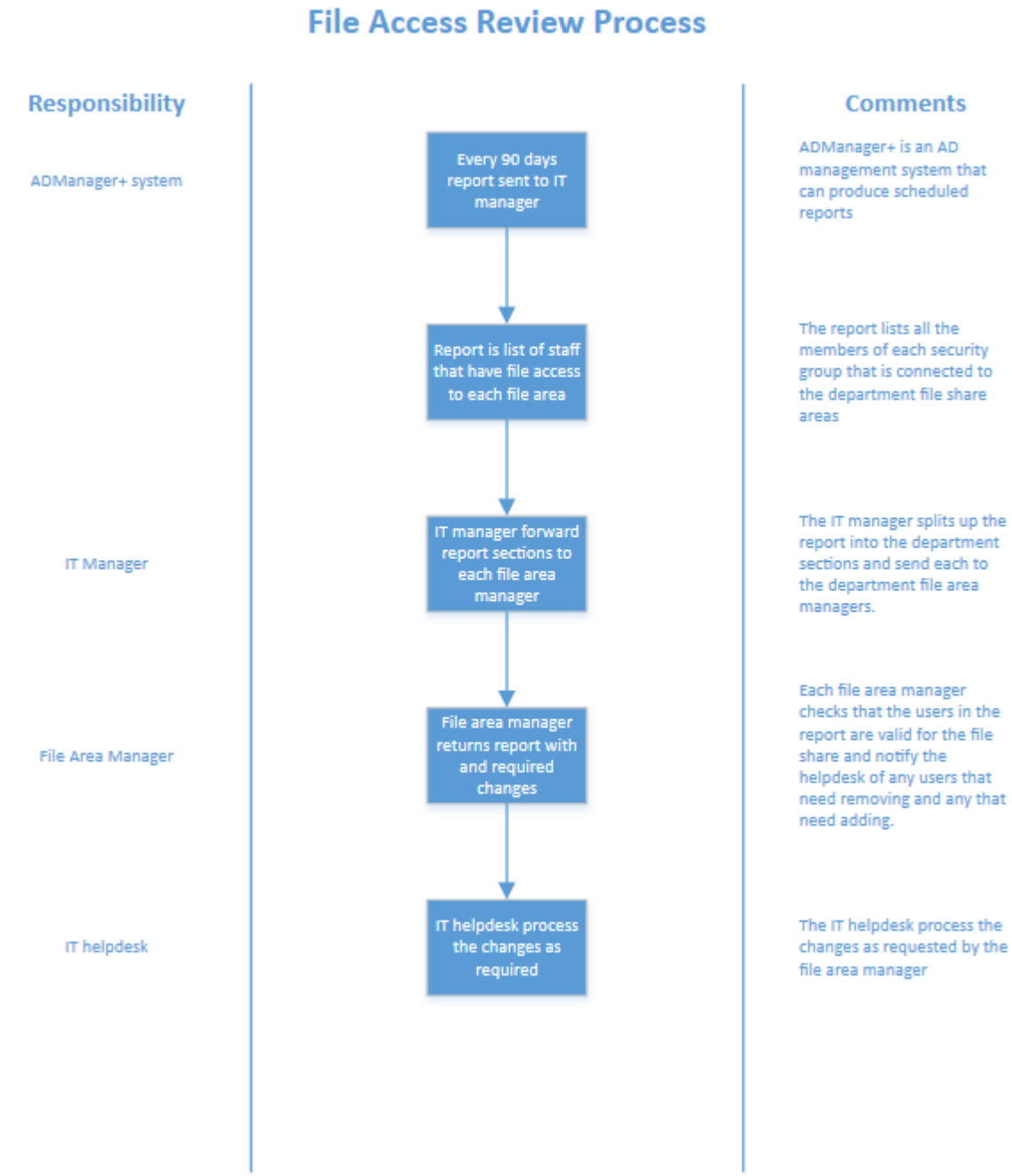
7 APPENDIX A

Staff Account Creation Process



8 APPENDIX B

File Access Review Process



9 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.