IT Acceptable Use Policy

Version 4.0

Version History

Version	Date	Description	Author
1.0	10/01/2015	Working Draft Version	Matt Beaver
2.0	13/01/2016	Approved by CMT & Governing Body	Matt Beaver
3.0	14/07/2016	Revised for OLASS	Matt Beaver
3.1	07/09/2016	Revised for IFT	Matt Beaver
3.2	24/01/2017	Revised for ISO 27001	Matt Beaver
3.3	04/04/2017	Added peer to peer, bittorrent exception	Matt Beaver
3.4	20/06/2017	OLASS exceptions checked and updated	Matt Beaver
4.0	**07/07/2017**	**Approved by Senior Leadership Board**	**Matt Beaver**

This document forms part of the Weston College Information Security Management System (ISMS).

1.0 Introduction

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

To use the Weston College Group **IT Resources, Users** must agree to the responsibilities and conditions outlined in this IT Acceptable Use Policy.

If you do not agree or understand any aspect of this policy you must logout, disconnect or stop using the **IT Resource** immediately.

1.1. Scope

This policy covers:

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

2.0 Legal Responsibilities

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 1998
- 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)

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

- Software / Website Licence Agreements
- Software / Website Terms & Conditions
- Copyright Agreements

1.1 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

2.0 User Accounts & Access Control

Access to The Weston College Group **IT Resources** are available via a **User Account** associated with an individual user.

Line Managers request **User Accounts** for staff via the New User Request Form on SharePoint.

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

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

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

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.

Access to additional **IT Resources** may be requested by systems owners by contacting the IT Helpdesk (it.helpdesk@weston.ac.uk | 01934 411425).

Access to **IT Resources** may be removed by system owners by contacting the IT Helpdesk (it.helpdesk@weston.ac.uk).

An IT helpdesk call will be raised for all permission changes as an audit record.

Management of access permissions is monitored and reported upon following the IT Permissions Monitoring & Reporting Procedure.

Shared or Generic **User Accounts** are not permitted.

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.

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

2.1 Special Access / Administration Access

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

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

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

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

2.2 Offender Learning

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

3.0 Passwords & Authentication

User Account passwords must meet the following requirements:

Passwords must be a minimum of 8 characters long

Passwords must not contain the **User's** First, Middle or Last Names

Passwords must not have been used before

Passwords must contain characters from three of the following five categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

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

Passwords must be changed every 60 days.

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

Users take full responsibility for any activity which takes place while logged in using their User Account.

3.1 Offender Learning

Passwords must be changed every 60 days. OLASS Account Creation Procedure.

4.0 Data Security

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 of time.
- 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.

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.

5.0 Monitoring and Logging

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

Monitoring and logging includes:

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

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

5.1 Safeguarding and Prevent

The following activity is actively monitored and logged as part of the Colleges responsibility towards multi-agency safeguarding and PREVENT agendas.

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

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.

5.2 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)

6.0 Vandalism

Acts of vandalism are taken very seriously. Anyone caught causing an act of vandalism will result in disciplinary or legal proceedings.

Any costs incurred repairing or replace vandalised equipment will be charged to anyone caught causing damage.

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

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

7.0 Software

Installation of licenced and approved software applications can be arranged via the **IT Helpdesk**.

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

7.1 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)

8.0 Viruses & Malware

The Weston College Group use a number of security systems to protect data and **IT Resources** from viruses and malware.

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

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

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

9.0 Internet Access

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**.

The Weston College Group **Social Media Policy** details access to social media websites and the additional responsibilities which you must accept by accessing these sites.

The Weston College Group **E-Safety Policy** and the **Anti-Bullying and Harassment Policy** detail acceptable online behaviours and electronic communication.

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 content is not filtered does not mean it is OK to access.

The College monitors and logs all usage of the Internet.

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

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

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

Users must not connect or tether to any devices while on a Weston College campus or site.

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

9.1 Higher Education

Staff and student 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:

- Staff and student HE users should not deliberately or knowingly seek to access material that is illegal and/or without proper licensing.
- Staff and student HE users confirm that in accessing any specific site, it is in connection with the academic requirements of the HE programme, and is for educational purposes only.
- Staff and student HE users 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.

9.2 Offender Learning

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

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

10.0 Remote Working

All Weston College mobile devices require completion and agreement to the terms of the equipment loan form before they are issued. All devices must be collected in person, devices will not be issued to 3rd parties.

Staff are reminded to assess their environment and position of screens to ensure any documents or data classified as “Internal Only” or “Confidential” cannot be viewed.

Staff are reminded that mobile devices 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.

All Staff issued mobile devices are issued with drive encryption enabled to help protect loss of data from theft. **Staff are reminded that drive encryption is only effective if the thief does not have access to or cannot obtain or guess the users password.**

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

11.0 Own Devices

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.

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

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

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.

Bring Your Own Network (BYON) is not permitted.

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

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

11.1 Offender Learning

Personal IT devices are not permitted to be connected or used within Offender Learning classrooms.

NOMS approved personal storage devices are permitted to be used on the Offender Learning networks as long as they meet all Weston College Group, NOMS and prison policies and guidelines.

12.0 Data Security, Removable Media & Backups

Data containing personal information or information which could be used to identify an individual must not leave the College Network by any means including:

- Email
- USB drives
- CD/DVD
- Cloud Storage
- Unencrypted laptop

It is the **Users'** responsibility to ensure personal information is adequately protected. Failure to do this may result in disciplinary or legal action. For advice on protecting data, please contact the **IT Helpdesk**.

All data must be saved to the College servers. Saving data to local storage devices is not permitted.

All data saved to the Weston College Group servers is securely located and backed up as detailed in the **Data Backup and Retentions Policy**. Please contact the **IT Helpdesk** to recover data from backups.

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

12.1 Offender Learning

Data must only be transferred between Prison IT systems using a single, prison approved, hardware encrypted USB flash drive.

The USB flash drive must be scanned for viruses on a Weston PC with up to date Virus definitions prior to transferring data to or from the Weston network.

Any resources being copied to the Weston network must meet NOMS and Weston IT policies.

All data backup schedules and storage methods are described in the OLASS IT Security Procedure 3.5. Please contact the **XMA Helpdesk** to recover data from backups.

All **IT Resources** must be connected to the Weston Education Domain by an XMA engineer or member of the server team. Any **IT Resources** not connected to the Weston Education Domain must be reported to the IT Helpdesk.

Laptops / mobile devices must not be used within the Prison estates. Any use of Laptops / mobile devices should be reported to the IT Helpdesk.

13.0 Remote Working

IT Resources may be available for **Users** to take off site. The Loan Equipment Form must be signed agreeing to the terms and conditions of the loan before any **IT Resources** are taken off site.

It is recommended that **Users** check that loaned **IT Resources** are covered by home and car Insurance policies in the event of theft. **IT Resources** should never be left in unattended vehicles. Costs to replace or repair damaged or lost **IT Resources** may be reclaimed from the **User**.

IT Resources should never be used while driving.

Special considerations should be made to data security when working away from the College. Data containing personal information must not be taken out on the College unless encrypted.

Data encryption for loan equipment is available so please discuss your data encrypting requirements with the **IT Helpdesk**.

Remote access to the College network is available via equipment purchase by the IT Department only. VPN access is not available for personal devices.

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

Sub-loaning of **IT Resources** to other **Users** is not permitted.

14.0 IT Resource Requests & Disposal

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

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

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

All **IT Resources** must be disposed 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.**

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

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

If **IT Resources** need to be reallocated they must be returned to the IT Helpdesk first for reallocation

15.0 IT Support

All issues with IT equipment or systems must be reported to the IT Helpdesk.
All IT issues and requests are logged and tracked to resolution.

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

15.1 Offender Learning

Offender Learning Users should follow the OLASS IT Support Procedure.

16.0 Definition of Terms

- **IT Resources** – include Computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, equipment, software, services, systems, Access to WIFI, etc.
- **Users** (Enrolled students, members of staff and associates)
- **User Account** (username & password used to login to the Weston College Group network)
- **IT Helpdesk** – Support desk for IT services contact 01934 411425 | it.helpdesk@weston.ac.uk

17.0 Related Documents

- IT Security Policy
- IT Backup and Retentions Policy
- IT Software Development Policy
- IT Disaster Recovery Plan
- Business Continuity Plan
- Financial Regulations
- Procurement Strategy
- Anti-Bullying and Harassment Policy
- E-Safety Policy
- Social Media Policy

- JANET Acceptable Use Policy

18.0 Approval & Review

Version : v4.0
Approval : Approved
Review : July 2018