

The Adult College of Barking and Dagenham

IT Acceptable Use Policy

Lead Responsibility	Service Manager Business Support
Designated Officer	Network Services Manager
Advisory Officer(s)	N/A
Approved by	Service Manager Business Support
Date of approval	September 2023
Date of next review	August 2024

A note to all teaching staff:

Please click [here](#) using a curriculum device to find a full list of Work and Skills policies & procedures

Please click [here](#) using an LBBB device to find a full list of LBBB policies

Purpose & Scope

The College seeks to promote and facilitate the proper and extensive use of Information Technology (IT) for the sole purpose of supporting the teaching, learning, and the employment activities of the college. This policy document details acceptable use of the College's IT equipment and services and provides a framework governing the use of all IT resources across all sites on which the college operates.

This policy applies to all users, including staff, learners, apprentices, delegates, visitors, contractors, partners, and others. It also addresses the use of the College's IT facilities accessed via resources not fully owned by the College, such as partner and service user's personal devices and equipment.

The IT facilities include hardware, software, (Office 365 applications) and data, storage, network access, telephony, printing, back-office systems, and services provided by third parties including, online, Cloud and hosted services.

The Adult College has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'Prevent'. The purpose of this duty is to aid the process of preventing people from being drawn into terrorism.

It is the responsibility of all users of the College's IT services to read and understand this policy. This policy will be updated to comply with legal and policy requirements, and it is your responsibility to keep up to date with any changes.

The College provides computers, mobile devices and networked resources for staff and learner use. The primary purpose of these services is to provide relevant resources to assist staff, learners, apprentices/delegates volunteers, guests, and governors whilst they work and study. Assistance in using all these resources is available from the Student Services Team and the Network Services department.

It is the policy of the Adult College to respect all computer software copyrights and adhere to the terms and conditions of any license to which the College is a party. The downloading and/or installation of unauthorised software and screensavers is expressly forbidden. This includes software downloads from the Internet and from email & Microsoft Teams. The College will not condone the use of any software that does not have a license and any member of staff or learner found to be using, or in possession of, unlicensed software will be the subject of disciplinary procedures.

Responsibilities

Please note that you are required to agree to this Policy before you log in to the College's network, onsite or remotely and/or accessing College emails/Teams on college or personal mobile devices. A written copy can be obtained from reception or the Network Services Department.

The College network is defined as all computing, telecommunication, and networking facilities provided by the College, with reference to all computing devices, either personal or College owned, connected to systems and services supplied on-premises or remotely.

By using a computer, mobile device, telecoms equipment or network services/Office 365 applications (MS Outlook, Teams, OneDrive, Yammer) or any other software belonging to the Adult College you are agreeing not only to follow the rules in this Policy but are also agreeing

to report any misuse of these services to the Network Services Department. 'Misuse' means any violation of this Policy, or any other use that is not included in the Policy and which has the effect of harming another individual or their property or breaking the law.

All users of the system must immediately report any suspected breaches, cyber-attacks, or security issues via the helpdesk [Helpdesk@Adult- College.Bardaglea.org.uk](mailto:Helpdesk@Adult-College.Bardaglea.org.uk) or on 020 8270 4722.

Individuals who handle personal, confidential, or sensitive information must take all reasonable steps to safeguard it.

The conduct of all users when using the College's IT facilities should always be in line with the College's Values, including the use of online and social networking platforms.

Users must not:

- Allow anyone else to use their user ID to access any college system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access college systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to IT systems or information, including changes to settings, the installation or removal of software and alterations to hardware or connectivity.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-authorized device to the College network or IT systems without prior permission from the IT Department.
- Share their personal details on any of the college platforms (Outlook/MS Teams), this includes and is not limited to mobile numbers/email addresses/D.O. B / home address etc.
- Give or transfer The Adult College data or software to any person or organisation outside without the authority of the Network Services Department.

Internet and email/Teams/Office 365 Conditions of Use

The Adult College has a duty of care to filter all web content to ensure its users are protected against unsuitable content including, but not limited to adult material, gambling, drugs, offensive, hate, discrimination, racism, violence, terrorism, and extremism. Attempting to access or bypass filtering to access this content will be deemed as unacceptable use for which users will be subject to college disciplinary procedures.

Use of College internet and email/Teams is intended for college business, study, and research. Occasional moderate personal use is permitted where such use does not affect the individual's business/learning performance, is not detrimental to the college in any way, does not breach of any term and condition of employment or learner agreement and does not place the individual or the college in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email/Teams/Office 365 systems.

Please note that MS Teams lessons are recorded for the benefit of learner revision and catch-up purposes only.

Users must not:

- Use the internet or email/chat for the purposes of harassment or abuse.
- Use the internet or email/chat to access or share any material that may be considered to relate to terrorism or extremism, nor should such material be downloaded or stored on systems owned or controlled by The Adult College.
- Use internet or email/chat to engage in or support the radicalisation or potential radicalisation of any individual, whether that person(s), known or unknown are within the college or not.
- Download or share on social media any lesson content which has been recorded for revision or catch-up purposes. It is a violation of privacy and GDPR regulations to share this content with any person outside of the College.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which The Adult College considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libelous material.
- Use the internet or email/chat to make personal gains or conduct a personal business.
- Use the email/chat systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to The Adult College alter any information about it, or express any opinion about the College, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email/chat on behalf of The Adult College unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.

Plagiarism, Collusion and Artificial Intelligence (AI)

Plagiarism, Collusion and Artificial Intelligence (AI) misuse are very serious offences and any learner found to be copying another learner's work; quoting work from another source without recognising and disclosing that source; buying in an assignment from a third party to pass off as their own either in part or totally; or using Artificial Intelligence software to generate in part or totally an assessment without correct citation and against the Adult College guidelines will be subject to college disciplinary procedures.

PREVENT

Learners and staff must not create, download, store or transmit unlawful material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Systems are in place to detect this type of activity and will be reported to the Safeguarding team.

Social networking is blocked in the College so the risk of radicalisation via these networks is reduced. Users who attempt to bypass college security (by using TOR Browsers, ultrasurf plug in) will be subject to college disciplinary procedures.

Monitoring and Filtering

The Adult College monitors and records the use of its IT facilities (all internet access is filtered and monitored; E-mail usage is monitored, and other IT system logging takes place where appropriate) for various purposes including:

- The effective and efficient planning and operation of IT facilities
- Detection and prevention of infringement of this policy, related procedures, and relevant legislation
- Investigation of alleged misconduct
- Compliance with lawful request for information from government and law enforcement agencies.

Any attempted breaches are automatically reported to the Network services Department and safeguarding team. Inappropriate use is subject to disciplinary procedures.

From time to time a staff member or learner over the age of eighteen may need access to materials that would otherwise be deemed as unsuitable for the purposes of study and research. A request stating the reason and the type of content required must be forwarded to the IT Department via Helpdesk@Adult-College.Bardaglea.org.uk who will seek authorisation from a member of the Senior Management Team to make the decision whether to allow such access and the permitted time.

Help and Assistance

It is important that you understand your responsibilities, so if you are unsure about what is allowed always speak with a member of staff.

If you require help using the College network, please speak to a member of staff at reception or contact the helpdesk at Helpdesk@Adult-College.Bardaglea.org.uk

If you notice someone using the College's IT equipment and network inappropriately, please inform a member of staff or the IT Department on (020 8270 4722 ext. 3131) or by email to Helpdesk@Adult-College.Bardaglea.org.uk or visit either of the college sites.

Equality and Diversity Impact Measure

The college has considered the Equality and Diversity implications in relation to the rules and policies set out in this document and does not consider them to unduly impact upon any protected group.

Legal Context

Data Protection Act 1998, General Data Protection Regulations (GDPR) 2016/679; and the Counterterrorism and Security Act 2015 (The Prevent Duty).

Location of Policy

Curriculum network via MS Teams: IT Advice/Help>General>Files>AUP

Version	Date	Status & changes	Author
0.8	15.09.23	Reviewed by Service Manager Business Support – Yvonne Bennett	J.S.Aujla