



## Equality Impact Assessment

Whenever a policy is reviewed or changed, its impact assessment also must be updated. The Equality Act 2010 seeks to simplify discrimination law and introduced statutory duties to promote equality whereby The College of West Anglia must, in the exercise of its functions, pay due regard to the need to promote equality in relation to the protected characteristics.

**Could any staff or students be adversely impacted by this policy/process? If yes give details and how this will be mitigated: No**

Date	Action and Monitoring:
30/01/2024	No Action required

### E, D & I Statement

This procedure has been reviewed in line with the Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment., Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation and Disability. We will continue to monitor this procedure to ensure that it allows equal access and does not discriminate against any individual or group of people.

## Contents

1 Introduction .....	4
2 Complying with CWA policies and the relevant laws.....	4
3 Consequences of not following this policy .....	5
4 Reporting problems .....	5
5 Use of systems generally.....	5
6 Monitoring.....	6
7 Account security.....	7
8 Use of email .....	7
9 Use of internet.....	8
10 Printing .....	8
11 Storage and backing up data .....	8
12 Physical security of computers and related items.....	9
13 Bring Your Own Device (BYOD) .....	9
14 Removable storage.....	10
15 Related Policies.....	10

## 1 Introduction

The college offer an extensive range of IT systems across campuses and online for course related activities and drop-in purposes. This policy applies to all college students and describes what the college considers acceptable use of college IT systems and data by students. By reading, understanding and acknowledging this policy, you are accepting that you are aware of your responsibilities and your acceptance will be recorded at induction. There will also be occasion where you will be reminded of this obligation in tutorials or other student events.

Students on Open University Collaborative Provision programs are required to follow this policy, relating to their interactions using IT systems at this institution in addition to the relevant OU policies, as outlined in your Conditions of Registration. Students should also ensure they have read and understood The Open University [Student Computing Policy](#), and [Social Media Policy](#). If you need any help or advice, please contact the college IT Service Desk in the first instance.

## 2 Complying with CWA policies and the relevant laws

All college students must comply with this policy, any related policies and laws governing the use of IT systems in general. This related legislation includes:

- Computer Misuse Act 1990; and
- Copyright Designs and Patents Act 1988.
- General Data Protection Regulation 2018.
- [Student Behaviour Policy](#)
- [Safeguarding, Child and Vulnerable Adult Protection Policy](#)

### 3 Consequences of not following this policy

Failure to acknowledge and adhere to this policy, and any related policies including the Student Behaviour Policy, will result in your access being removed and may result in you being removed from the college whilst an investigation is carried under the college disciplinary process. Any action deemed to be criminal will be reported to the relevant authorities. This includes but is not limited to:

- Accessing or attempting to access any college system to which you have no access rights.
- 'Hacking' or attempting to 'hack' any college account where strict permission has not been given. This includes email accounts.
- Introducing or attempting to introduce any foreign software to the detriment of the college network and associated systems.
- Physical intentional damage of IT resources.
- Cyber bullying and harassment.
- The use of IT to create, share or distribute offensive content.
- Violent or extremist activity that may lead to potential terrorism.

### 4 Reporting problems

The IT Services department is available to assist you. If you become aware of a security incident e.g. someone attempting to gain access to information they are not entitled to, or a problem that has the potential to become an incident, you should report these to the IT Service Desk immediately via telephone on 01553 815325 or email [ITServiceDesk@cwa.ac.uk](mailto:ITServiceDesk@cwa.ac.uk)

### 5 Use of systems generally

IT systems are provided for use to all college staff and students to enable them to carry out their normal day to day tasks. This should be done with due consideration to other users of the IT systems so as not to prevent them from carrying out their work and subject to the following conditions.

- All IT systems should be treated with respect and not moved or modified unless you have been authorised to do so.
- College IT systems should not be used for recreational purposes during lessons, personal business use or other non-college related matters unless you have been expressly authorised to do so. The college reserves the right to stop non-college related activity where this is impacting service.

- If the system you need access to is unavailable please log a call with the IT Service Desk.

### **IT systems must not be used to:**

- Gain unauthorised access to systems or data that you have not been granted specific access to.
- Create, access, store, use, copy or distribute inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures or videos that might cause offence or embarrassment.
- Create, transmit or access unauthorised or copyrighted software or copyrighted material. The Copyright, Designs and Patents Act 1988 states that only the copyright owner is allowed to use the information. Any reuse of downloaded information without permission is prohibited this includes music piracy.
- Allow unauthorised people to use college systems or access College data within systems, either on-site or remotely.
- Deliberately introduction of malicious programs into the network, file servers or workstations (e.g. viruses, scanners, 'hacking' tools, password crackers, etc.); and
- Remove any preinstall software from college owned devices.
- Install or download any software on college owned devices which is not licensed for use in college. Any software that is required must be installed by, or with consent of, the IT Department.
- Enable cheating, plagiarism or falsification of work, or activity that in any way constitutes malpractice or breaches academic regulations of the college and partner institutions.

## **6 Monitoring**

In order to comply with the college's prevent and safeguarding responsibilities, the college has installed software on all college owned devices that will monitor user activity and assist us in identifying potential concerns. Such software will not record every action but may record any activities considered to be indicative of risk. All user internet access is also recorded and stored securely for up to 12 months.

## 7 Account security

It is the responsibility of each user of college IT systems to protect their user account details and observe the following.

- Do not share your username or password with anyone else.
- Do not write the details down or store them electronically except in an encrypted form.
- Do not email your password to anyone or reveal it to anyone under any circumstances;
- Do not use the same password for college IT systems that you use elsewhere; and
- Do not attempt to use someone else's logon details.

When the individual leaves the college their accounts in the various systems provided by the college will be disabled (after 31<sup>st</sup> Oct in the year they were enrolled to enable collection of certificates via Student Portal and to avoid unnecessary complexity for returning students).

## 8 Use of email

College email is provided to enable students to communicate with fellow students, college staff and others outside of the college, on college related matters. It is subject to the restrictions outlined in 'Use of systems generally' above as well as the following, The General Data Protection Regulation 2018 and email specific restrictions:

- College provided email accounts should not be used for personal communications and college email addresses should not be provided to third parties not involved in college related activities;
- Students should check their email at least once a week.
- Spam, unsolicited bulk or marketing materials or nuisance emails must not be sent from college email addresses and if you receive such unsolicited messages, please report them to the IT Service Desk.
- Do not open messages or attachments from unknown senders.
- Do not send messages on others' behalf or attempt to forge emails.

The college reserves the right to access, review, copy, delete, disclose or use student email files at any time and without notice. Student emails can be monitored in line with privacy legislation, without prior notification, if it is deemed necessary for the purpose of ensuring this

policy, or related policies are being adhered to. Upon leaving the college your college email account will be terminated and all emails removed.

## 9 Use of internet

Internet access is provided for college related use, personal and recreational use is only permitted where expressly authorised. All internet use subject to the restrictions outlined in 'Use of systems generally' above.

Use of social media is generally accepted, although this should be outside of class unless expressly permitted by the tutor. Students should be aware that the student code of conduct extends to use of social media both onsite and offsite.

The college does not tolerate bullying, abuse or discrimination and this applies equally to email and other forms of electronic communication, including social media platforms. Any issues brought to The colleges attention will be dealt with via our disciplinary procedures, even if not directed at college staff or students

The college maintains the right to monitor the volume of internet traffic generated, together with the internet sites visited by individuals, to investigate excessive or inappropriate use and to block web sites it feels are inappropriate. This includes encrypted SSL (https://...) based internet sites which will be inspected by decrypting and inspecting the page contents. The only exception to this is internet banking websites and some exam services;

Attempts to access restricted content, even if blocked by the college firewall, are automatically alerted to college management. As such, if you accidentally access a site containing inappropriate material please report this to your course director.

With so much information available online, it is important that students learn how to evaluate internet content for accuracy and intent. Students will be supported to develop and improve these skills via the iCWA programme.

## 10 Printing

Students are charged for printing and can obtain print credit from various locations dependent on campus attended. To find out more about printing please ask at any reception or student services location.

## 11 Storage and backing up data

Student storage is now within a college provisioned Microsoft OneDrive, this can be a useful method of storing files to be accessed both in college and at home. Network storage is no



longer available.

It is the responsibility of all students to ensure that they backup their documents to their own devices and take sufficient precautions of their own to ensure files are not lost.

Some students will still be required to save some of their work to the local network storage depending on what courses they are undertaking. These students will be advised on where they need to store this data. Upon leaving the college you should not expect your data and coursework stored on the college network to be retained for more than 3 months. Data held within their college provisioned OneDrive account will be kept for 12 months after completing their course, if access is required after 3 months of leaving the college, contact with Student Services will be required to facilitate access. After 12 months the files will be deleted permanently.

## 12 Physical security of computers and related items

Please make sure you leave any college provided computers in a secure location. If you are the last to leave a room lock the door if you are able to or locate someone who can.

Do not leave mobile computers or removable storage devices unattended.

If you notice anyone acting suspiciously or wandering around the college campus without identification then report it to a member of staff immediately.

If you believe a computer has been damaged or stolen report it to the IT Service Desk immediately.

## 13 Bring Your Own Device (BYOD)

The college allows you to use your own computing device, including mobile phone, to access the college network subject to the following conditions.

- You can only connect your device to the college wireless network, using instructions provided by the IT Service Desk;
- Users should not setup mobile hotspots as these may interfere with the performance of college Wi-Fi;
- It is your responsibility to make sure your device's software is up to date and the operating system updates are applied; and
- Where supported by the operating system, an up-to-date anti-virus application should be installed and working; and
- No device with compromised operating system, such as "jailbreak" or "root"

access should be used to connect to college systems.

- When charging devices in college, users must take responsibility to ensure that cables are of a suitable standard. USB charging facilities are available in various locations and should be used where possible. Portable Appliance Testing (PAT) is available via the LRC (Learning Resource Centre).

The college offer facilities to store and charge personal devices at various locations across our campuses. All belongings are left at the individuals own risk and the college accepts no responsibility for any loss or damage incurred as a result of using these. The lockers are available for short term storage and should never be used for overnight storage, anything left overnight will be removed and will need to be claimed from lost property.

## 14 Removable storage

Removable storage, which includes devices such as external hard drives, USB memory sticks and SD cards, may be used in college for the temporary storage and transfer of files and documents to and from the college network subject to the following conditions.

- Removable media must be virus scanned when connected;
- Do not attempt to disable or by-pass the virus scanning; and
- Do not leave any removable devices connected to college computers.

Please be aware that college virus protection may automatically delete or quarantine file which pose a risk to college systems. The college accepts no responsibility for loss of files

## 15 Related Policies

- [Student Behaviour Policy.](#)
- [Safeguarding, Child and Vulnerable Adult Protection Policy.](#)
- [ICO guidance on GDPR](#)
- [Student Charter and Code of Behaviour](#)
- [Assessment, Internal and External Quality Assurance Policy](#)