IT ACCEPTABLE USE POLICY
2023 - 2024

Date Approved	February 2023
Approved By	Finance and Strategy Committee
Review date	March 2024
Responsibility	Director of IT and Network Services

Acceptable Use Policy

Content

INTRODUCTION

Sandwell College Group seeks to promote and facilitate the proper and extensive use of Information and Learning Technologies (ILT) in the interests of teaching and learningand in support of the business needs of the organisation.

The College’s intentions for publishing an Acceptable Use Policy are not to impose restrictions on a culture of openness, trust and integrity, but to protect its employees, students, partners and the organisation from illegal or damaging actions by individuals, either knowingly or unknowingly.

PURPOSE AND SCOPE

This Policy defines the acceptable use of all Information and Learning Technologies within in the Sandwell College group of colleges. It applies to:

- all staff, learners, Governors, contractors, consultants and others who use its services, wherever that use may occur
- all computing, telecommunication, networking and audio-visual facilities, equipment and resources
- all classrooms, workshops, Learning Hub/Centres and offices where the above resources are located
- all institution data and information systems
- all institution licensed software
- all on-line services and resources
- Bring your own device (BOYD)

This policy is taken to include the following Policies:

- JANET Acceptable Use Policy
- Combined Higher Education Software Team (CHEST) Code of Conduct
- Safeguarding Policy
- e-safety Policy
- Data protection policy
- Any other user terms and conditions which are part of an on-line database to which the College subscribes or has use (FENC, NLN etc)

College Policies are available on the staff Sharepoint Hub for Staff and Virtual College for Students

This policy is also in place to make users aware of their duty to use college computer and network resources responsibly, professionally, ethically and lawfully.

ROLES AND RESPONSIBILITIES

It is the responsibility of the Governors, through the Executive Team, Senior Management Team and College managers, to ensure the effectiveness of and compliance with this policy. It is the responsibility of all members of the College to adhere to the provisions of the policy and to ensure that ILT and the Internet providesa safe method of working.

The responsibility for the supervision of this Acceptable Use Policy is delegated to the Director of IT and Network Services

SECURITY

Passwords must be kept secure and **accounts must not be shared**. All users are responsible for the security of their passwords. They should be changed in line with the Password Policy.

Additional care should be taken with portable devices.

Only College owned computer equipment may be physically connected to the network. College member's and visitor's own devices can be connected using the appropriate wifi network and passwords.

PORTABLE APPLICATIONS (e.g. Portable Firefox) may **NOT** be used without prior permission of the Network Team

Users should be cautious when opening e-mail attachments from unknown senders in case they contain viruses or malware.

Security measures should not be revealed to others.

The College uses firewalls and virus protection as part of its security measures and all incoming e-mails are scanned.

Filtering software is also in use.

ACCESS

The Internet and ILT resources are accessible to all members of the College, regardless of age, race, gender, religion, background or disability.

The College Virtual Learning Environment, Sandwell Virtual College (SVC), is available to all members remotely.

Access to computer equipment is via the College Learning Hubs. A booking system is in use for Open Access PCs.

Other ILT equipment can be booked via the Learning Centres. (examples: digital cameras, digital video cameras). These can be for use in the Centre, in classrooms, Learning Bases, or off-site for supporting the work of the College.

The college reserves the right to block internet access to sites which it deems do not support the primary business of the organisation.

Help and support for using the resources is available via the Learning Centres and the ILT Helpdesk.

College members and visitors are able to connect their own devices to the wifi network using the appropriate log in and passwords.

USE OF BYOD

The College supports BYOD and provides WIFI access to Staff and Students via the eduroam service. Guests can request temporary access by contacting the ILT Team

As part of the software licensing agreements, staff and students can download Microsoft Office 365 on to their personal devices. College staff are able to access Microsoft Office and windows applications for their personal devices, subject to certain restrictions. For both the above, the resources are only available whilst a student or an employee of the College.

Owing to a lack of power outlets and the need for all devices to have been electrically tested by the College, The college is unable to offer access for users to charge their devices. It is necessary for users to ensure their devices are charged sufficiently for their planned use before they come in to College.

PRIVACY

The Network Team, facilitate access and monitor activity of all IT and Network services. Strict controls are on place to ensure access is only granted to those with a legitimate requirement. Responsibility is extended to all staff to maintain the highest levels of privacy for the data that they are authorised to access.

The College fully reserves the right to monitor e-mail, telephone, internet access and any other electronically mediated communications, whether stored

or in transit, in line with its rights under the Regulation of Investigatory Powers Act 2000.

Access to staff files will have to be initially approved by a member of the Senior Leadership Team. If feasible and appropriate the permission of the member of staffwill be sought.

Access to student files and e-mail will be approved by a member of the Senior Leadership Team. If feasible and appropriate the permission of the student will be sought.

Reasons for this may include the need to:

- Ensure the operational effectiveness of services
- Prevent or investigate a breach of the law, this policy, or another College policy, suspected breach of examination board regulations, issues to do with plagiarism etc.

If a member of staff leaves the College, any files which are left on any computer system owned by the College, including servers and electronic mail files, will be considered to be the property of the College.

When a student leaves the College, stored files will be retained for a period of six months after their leaving date and will then be deleted. Student e-mail accounts willbe disabled immediately on leaving.

Assignments submitted to the VLE will be retained for the current year plus one. Learners requiring copies of assignments from the previous year need to contact their tutors.

Sandwell College reserves the right to access the history of usage of a computer and to use results in any disciplinary hearings. This applies to bothstaff and students.

ACCEPTABLE USE

Acceptable use of the college's IT/ILT information systems, resources and facilities is defined as their use in support of the organisation's teaching, learning andadministrative activities, and which does not come under the category of prohibited orunacceptable use.

Acceptable use is that which is necessary in furtherance of a course of study or employment with the College and which is not prohibited.

For **students**, this includes:

- research and assignment work,browsing for information, downloading relevant facts and
- using on-line databases and other resources to which the College subscribes
- access to the College Virtual Learning Environment.

For **staff**, this includes the above in all administrative, teaching and research/studyactivities.

Both staff and students are able to use the on-line resources, including e-mail, of the College for personal use.

Staff personal use must always be reasonable, not excessive and must not detract staff from their work. Personal use of more than 45 minutes per day may be seen as excessive. Such personal use should not be at a time when other users require the equipment for business use and must not be during working hours (i.e. personal use must only be in agreed break/lunch periods).

STORAGE ON THE COLLEGE NETWORK

All members of the College have space allocated to them to store work related documents.

Storage space is limited and therefore significant volumes of **personal** files such asMP3/4, video and large files of photographs must not be stored on College facilities.

The personal files for any user must not exceed 50Mb and the college takes no responsibility for such files. Any personal files must be stored in a folder named“Personal”.

The College will monitor the storage volume of users and will contact those withunexpectedly high volumes of storage.

Files stored on the network should not infringe any copyright or any other law.

Only files of the types defined within the **Acceptable use** definition should be storedon the network.

Disciplinary action may be taken against any staff or student who store files of the types defined within the **Unacceptable Use** criteria.

E-MAIL

E-mail is provided for staff and students for work related and personal use within the limitations above. E-mail usage is monitored by the College and inappropriate use is subject to disciplinary procedures.

UNACCEPTABLE USE

Under no account is any user authorised to engage in any activity that is illegal under British or international law while using college resources. The list below is not comprehensive, but attempts to categorise some activities which comprise unacceptable use.

The network and the Internet, including e-mail where applicable, may not beused for any of the following:

1. the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecentimages or material;

2. the creation or transmission of material which is designed or likely to cause annoyance, offence, inconvenience or needless anxiety;

3. the creation or transmission of material or information which could be considered to be racially abusive, or which contravenes any equality and diversity laws or College codes of conduct;

4. the use of any networks or equipment within the College, or directed at College members, which is intended to frighten, embarrass, or harass an individual (cyber bullying, cyber harassment, cyber threatening);

5. Any action or transmission which is in contravention of the College's Safeguarding Policy;

6. the creation or transmission of defamatory material;

7. the transmission of material such that this infringes the copyright of another person;

8. any anti-social or unacceptable use of the e-mail system: passing on chain mail, spam, hoax virus warnings etc;

9. unsolicited advertising (spamming);

10. deliberate unauthorised access to other computers of networks illegally or without permission;

11. deliberate activities with any of the following characteristics:

    - wasting staff time or networked resources;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the Internet in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);

12. continuing to use an item of networking software or hardware after thecollege has requested that use cease because it is causing disruptionto the correct functioning of the Internet or network services;

13. other misuse of the Internet or networked resources, such as the introduction of malicious programs into the network (e.g. viruses, worms, Trojan horses, e- mail bombs etc.);

14. where the Internet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use;

15. the unlicensed downloading, distribution or storage of music, video, film, or other material;

16. storage of personal data files (of any media type) that are not required for the legitimate delivery of college business;

17. the distribution or storage by any means of pirated software;

18. connecting an unauthorised device to the college network;

19. Plagiarism – the intentional use of others material without recognition; (Disciplinary procedures will be instigated for any breach or act of plagiarism.)

20. Any other action which is in contravention of the Computer Misuse Act 1990, which makes the following an offence:

    - to erase or amend data or programs without authority;
    - to obtain unauthorised access to a computer;
    - to “eavesdrop” on a computer;
    - to make unauthorised use of computer time or facilities;
    - to maliciously corrupt or erase data or programs;
    - to deny access to authorised users.

PREVENT

The college has a statutory duty, under the Counter Terrorism and Security Act2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

Members of the College community must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Systems are in place to detect this type of activity and are 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 (e.g. by using Tor Browsers, ultrasurf plug in) will be subject to college disciplinary procedures.

USE OF COLLEGE IT/ILT EQUIPMENT

It is the responsibility of all users to protect, maintain and secure all College equipment for the benefit of all.

Rooms containing equipment, including projectors, whiteboards, laptops, should be kept locked at all times when they are not in use. It is the responsibility of the user of the room to ensure this is carried out, which may include waiting for Buildingmaintenance to lock the room.

ALL staff are responsible for taking action to prevent the theft of portable equipment.

Ensure machines such as LCD projectors are turned off, and are turned off correctly,to prolong their life.

Ensure that all faults are reported so that the next person can make maximum use ofthe equipment.

Take additional care when using portable equipment off site and when transporting it.

Users must not cause any form of damage to the College's computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software. The term "damage" includes modifications to hardware or software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements may be charged to the individual or Department.

GOOD "HOUSEKEEPING" TIPS

Below are a few measures that all users should adopted to effectively support the smooth operation of the college IT resources.

- Keep your password(s) secure.
- Inform staff of any observed infringement of the use of the IT resources whether it be by learners or staff.
- Review files regularly and delete unused/unwanted resources.
- Never leave a computer logged when it is unattended. The user who is logged on to a computer is responsible for its use.

COMPLIANCE WITH THIS POLICY

- It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure thatunacceptable use of ILT services, resources and equipment do not occur.

- Unacceptable use by students or staff will, in the first instance, be challenged by tutors or line managers. Should the unacceptable use by an individual be of a serious nature, or be repeated, then the disciplinary procedure (student or staff) will be invoked.

THE LAW

The following Acts of Parliament are relevant to unacceptable use:

Copyright, Designs and Patents Act 1988
Malicious Communication Act 1988
Computer Misuse Act 1990
Criminal Justice and Public Order Act 1994
Trade Marks Act 1994
Defamation Act 2013
General Data Protection Act 2018
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Communications Act 2003