Myerscough College
Providing opportunities for all

Student Acceptable Use of IT Resources Policy and Procedure

It is the aim of Myerscough College to ensure legal compliance and the effective and efficient use of IT resources available to students.

This policy clarifies the basis on which IT resources are provided for students and the manner in which they may be used / accessed. This policy draws from and endorses the college Safeguarding and Prevent agenda and is in place to ensure its resources can be safely deployed.

The policy is applicable to all students at Myerscough College and relates to all IT resources provided by the College at all sites.

Procedure

Student Access and Use of the Student Computer Network

All students undertake an IT induction when starting their studies at Myerscough College. This Policy and Procedure is referenced during that induction and it is available via the student intranet.

Students accessing and using the student computer network, when either connected wirelessly or via a fixed connection, should do so in a responsible manner; at all times observing the College requirements within the legal framework. The following rules apply:

1. Behaviour

The computer areas are for work and, whilst some discussion may be necessary, students are required to keep noise to a minimum. If a member of staff considers student behaviour to be inappropriate or disturbing others, the student/s will be asked to leave.

2. Music

All computers with CD Drives will play audio CDs, however students must provide their own headphones. The use of speakers is not permitted and the volume on headphones must be set so as not to disturb others. Students are not permitted to listen to music whilst attending a taught class unless it is teacher assigned and an integrated part of the lesson.

3. Mobile Phones

In IT Drop-in areas, to avoid disturbing others, mobile phones must not be used to make/take voice calls. Use of a mobile phone at any time in a taught class will result in disciplinary action being taken. Please be aware that mobile phones emit electromagnetic radiation which may damage or otherwise corrupt the contents of hard disks or pen drives.

4. Software

The installation and/or downloading of software (including screensavers and multimedia players) onto College computers is not permitted. All software necessary for course work is supplied on the College network.

5. Virus Protection

The College has virus protection software running over the network, updated on a regular basis. However, the College cannot be held responsible for any damage to student files caused by the action of a computer virus. Students should take appropriate steps to ensure their own work and essential files are backed up securely.

6. The Internet and Email

Access to the Internet and e-mail is provided primarily for students to complete College related work. All internet sites that are accessed and all emails sent and received are logged and the computer and user ID can be identified at any time. The College does not permit any of the following on College provided computers and such conduct will lead to disciplinary action:

(i) viewing or forwarding of content deemed to be illegal, unacceptable or offensive to others eg pornography, offensive emails;

(ii) dissemination of material that may be considered libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery or impersonation;

(iii) the playing of computer games, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses);

(iv) downloading of multimedia files not related to coursework;

(v) downloading and / or infringement of copyrighted material.

(vi) Reference to filtering and monitoring

(vii) Reference to the Prevent Duty

(viii) Filtering as part of the College's duty to restrict access to harmful content including content which may draw people into extremism

7. Social Networking Sites

Access to social networking sites from the College estate is not restricted but all internet activity is logged and monitored. Whilst Myerscough College understands the popularity and usefulness of social networking sites to both staff and students, please be aware that if any of the following are found in the public domain, disciplinary action will be taken:

- The posting of any information, photos or other items online that could embarrass or defame the College. This includes information that may be posted by others on your page;
- The posting of any details, information, photos or other items that may cause embarrassment or offend members of staff. This includes information that may be posted by others on your page;
- Any posting that may infringe any of the College policies such as, but not limited to, Data Protection, Copyright, FREDIE, Student Anti-Bullying, Esteem in the Workplace, Safeguarding and Prevent.

For students' safe enjoyment of these sites please remember, before participating in any online community, that:

- Anything posted online is available to anyone in the world. Any text or photo placed online becomes the property of the site(s) and is completely out of your control the moment it is placed online - even if you limit access to your site;

- You should not post any information, photos or other items online that could embarrass you, your family, or the College. This includes information that may be posted by others on your page;
- Never post your home or college address, phone number(s), birth date or other personal information, the 'person' you're talking to may not be who or what you thought;
- When creating your profile, don't use details you may have used as a password or 'password reminder' on a banking site.

Students should be aware that they could face disciplinary action for violating College policies and that the Police and other law enforcement agencies monitor these websites regularly, as do potential employers as a way of screening applicants.

Communication may be established between staff and groups of students only by using approved and regulated tools such as the College VLE, Canvas, or the sanctioned College Social Media sites.

8. Consumption of Food and Drink

Food and drink is not permitted in computer areas and students will be requested to leave the area if found to be in breach.

9. Reporting Problems with a PC or Software

If IT support/assistance is required, including printing problems, this should be sought in the first instance from the following members of staff or locations:

Learning Resource Centre - Ground Floor (Fitzherbert-Brockholes)	Librarian/Library Staff
Drop-in Centre (First Floor Fitzherbert-Brockholes)	Service Desk Supervisor
Drop-in Centre (HE Centre)	Service Desk Supervisor (FHB)

NB: Members of staff should not be interrupted if they are teaching a class.

10. Logging On and Off the Network

Students are encouraged to ensure that computers successfully complete their start up routines as this enables the network checks to be carried out to ensure there are no missing or extra files required to enable the computer to perform at maximum efficiency.

Students are also encouraged to log off the network after completing their work or their study session.

11. Passwords

All users of computer facilities are required to keep their login passwords secret and not to allow others to use it. Students will be held responsible for all actions linked with their individual login and therefore it is recommended that a computer is not left unattended whilst still logged on.

Internet accounts are to be used only by the assigned user of the account for authorised purposes. Attempting to obtain another student's account password is strictly prohibited. A student may contact the Service Desk Supervisor to obtain a password reset if they have reason to believe that any unauthorised person has had access to their account and learned their password. Students must take all necessary precautions to prevent unauthorised access to internet services.

Students should change their passwords on a regular basis. Passwords can be changed or reset by registering for the service in the MyAccount area of Office 365.

12. Saving Work

All students are allocated 1Tb of Storage in Office 365 OneDrive. This is a cloud based service available independent of your location on a 24x7x365 basis. All student work should be stored here, under your own account. Files and data saved in OneDrive are backed up and can be recovered. A member of the IT Team can help with this on request.

On connecting to a College computer, a small mapped partition that presents as the n: drive. Is generated. This is used as a placeholder for the login in process and not available externally. The amount of storage allocated here is generally too small to be useful for storage of academic work and students are encouraged to use OneDrive.

The use of Pen Drives or USB data sticks is actively discouraged. This type of storage is very unreliable and susceptible to mechanical damage, malware attack, accidental loss or theft. Please do not use them to store any important data or as a primary back up device. Use your Office 365 account.

13. Printing

All students are allocated a number of printing credits, for use on any student printers. This should be sufficient to cope with the required printing for the student's course. When these are exhausted, further printing credits may be purchased.

The printing of objectionable material, whether text or graphics, artwork or photographic is not permitted and will result in disciplinary action being taken.

14. Residential Network (ResNet)

Residential students with access to ResNet must comply with the ResNet Conditions of Use.

15. Reference

All queries about this policy or its practical requirements should be made in the first instance to the Director of IT & MIS, who is responsible for the execution of this policy.

Documents Associated with this Policy

- FREDIE Policy and Procedure
- Student Anti-Bullying Policy (including Harassment)
- Esteem in the Workplace Policy and Procedure
- Data Protection Policy and Procedure
- Child Protection and Safeguarding Policy and Procedure
- Prevent Risk Management Plan
- Social Media Policy and Procedure
- Residential Network (ResNet) - Conditions of Use

Document History			
Author:	Director IT & MIS	**Ref and Document Version:**	Student Acceptable Use of IT Resources Policy and Procedure – V1
Approval:	College Executive	**Approval Date:**	December 2020
Review Date:	December 2023		
Publication:	Staff Intranet Student Intranet Website		
Quality Assurance			
This Policy and Procedure maps to the following external quality assurance frameworks			

Framework	**Framework Section Reference(s)**
Education Inspection Framework	
MATRIX	
QAA	
QIA	
ESFA	

Key Changes to Document
Minor amendments

All Myerscough College Policies are subject to screening for Equality Impact Assessment

Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, marriage or civil partnership, sex or sexual orientation

Myerscough College not only fulfils its legal position in relation to current and future equality legislation, but additionally goes beyond compliance in providing and promoting “Opportunities for all to succeed”, free from any aspect of discrimination, harassment or victimisation.

All staff have a duty of care to look after the interests of and support their colleagues. *This policy takes account of* our commitment to eliminating discrimination, identifying and removing barriers and providing equal opportunities for our learners, staff and visitors to ensure that no one feels excluded or disadvantaged.

Safeguarding, Learner Protection and Prevent

All staff have a responsibility to support and promote the College’s commitment to providing a safe environment for students, staff and visitors. Additionally, all staff have a responsibility to report any safeguarding or Prevent issues to the Designated Senior Lead for Safeguarding and Prevent.