EXPANSE LEARNING
PROGRESSION THROUGH EDUCATION AND CARE

ICT Acceptable Use Policy

Sept 2021

Version 5

1. Scope

This policy applies to all staff at Expanse Learning.

2. Introduction

Expanse Learning believes in the educational value of such electronic services and recognises their potential to support the curriculum. Every effort will be made to provide quality experiences for students and teachers using this service. Inappropriate and/or illegal interaction with any information service is strictly prohibited.

Students should not be able to access harmful or inappropriate material from Expanse Learning's IT system however; we will need to be careful that 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding. To qualify for Network, Internet and e-mail access, students must read, sign and return the agreement.

If British decency laws are breached or the Computer Misuse Act 1990 is breached then a student is likely to have the matter referred to other authorities including the police. The Computer Misuse Act 1990 identifies three specific offences:

- Unauthorised access to computer material (that is, a program or data).
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
- Unauthorised modification of computer material.

Please read this document carefully, only once the acceptable use agreement has been signed and returned will access to the computer system be permitted. Listed below are the provisions of this agreement. If anyone violates these provisions, access to the Network, Internet and e-mail will be denied and they will be subject to disciplinary action.

3. Personal Responsibility

As a representative of Expanse Learning, you will accept personal responsibility for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and attempts to disrupt or hack into the computer network.

4. Acceptable Use

The use of ICT must be in support of work activities, education activities and research in accordance with the educational goals and objectives of Expanse Learning. Everyone is personally responsible for this provision at all times when using any ICT resource. Use of other networks or computing resources must comply with the rules appropriate to that network. (e.g. within other partners of the group or when on work placement).

Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws. Use for commercial activities by for-profit organisations or personal enterprise is generally not acceptable.

5. Privileges

The use of ICT is a privilege and inappropriate use can result in that privilege being withdrawn. Students will participate in a discussion with a member of staff as to proper behaviour and use of the facilities. Staff will rule upon inappropriate use and may deny, revoke or suspend usage.

6. Network Etiquette and Privacy

Everyone is expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:

- *BE POLITE - Never send or encourage others to send abusive messages. Respect the rights and beliefs of others*
- *USE APPROPRIATE LANGUAGE - Remember that you are a representative of the group on a global public system. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.*

- *PRIVACY - Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.*
- *PASSWORD - Do not reveal your password to anyone. If you think someone has obtained your password, contact you're Line Manager/tutor immediately.*
- *ELECTRONIC MAIL - Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.*
- *REFERENCE WORK - Cite references for any facts that you present. Do not copy another person's work and imply that it is your own (i.e. plagiarism). Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.*
- *DISRUPTIONS - Do not use the network in any way that would disrupt use of the services by others.*

7. Services

Expanse Learning makes no warranties of any kind whether expressed or implied, for the network service it is providing. Expanse Learning will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, errors or omissions. Use of any information obtained via the network or other information systems is at the user's own risk. Expanse Learning specifically denies any responsibility for the accuracy of information obtained via its Internet services.

8. Security

If you identify a security problem, notify you're Line Manager/Tutor at once. Never demonstrate the problem to another student. All use of the system must be under your own username and password. Remember to keep your password to yourself. Do not share it. Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

Staff with their own assigned devise should use a password-protected screensaver to prevent unauthorised access to electronic records if you have to leave your computer unattended. It is critical that you **Log out and switch off your computer at the end of each day**, this allows your computer to install any critical updates that are required. In addition, ensure you choose a good password of at least 8 characters long, with a mixture of letters, numbers and symbols. Keep passwords secret.

9. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

10. Online Ordering systems

It is strictly forbidden for students to use the Internet for ordering goods or services regardless of their nature. In addition, it is also forbidden for students to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.

11. Electronic Mail

Electronic mail (email) is provided by the group (Office 365). The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence. Disciplinary action will be taken in all cases. It is also forbidden to send large volume emails (spamming).

12. Non-Educational Online Activity

Students are not permitted to access non-educational games, media (e.g. YouTube) or chat services available online, unless with specific consent from their tutor.

13. Microsoft Teams

Microsoft Teams has been implemented to be used for Online Learning purposes. The relevant Student/Teacher policies have been enforced and it must only be used in relation to the students learning activities. Students are not permitted to use Microsoft Teams outside of educational purposes for social reasons (e.g. for general socialising/chat). (Please refer to the Online Teaching Policy for further information. Microsoft Teams will be audited for misuse and any suspicious activity may be subject to disciplinary action.

14. Internet Search Engines

Students are required to use Internet search engines responsibly. If students are found to be searching for material unsuitable and in breach of this policy, they will face disciplinary action. Students are strictly forbidden from removing safety filters from Internet Search engines in order to access unsuitable material. This includes but is not limited to the removal of the default filtering feature.

15. Executable, Music and Video Files

Staff and students are strictly forbidden from introducing executable files (e.g. '.exe, .cmd, .bat, .bin') to the network as these can is some cases contain harmful viruses. This includes but is not limited to copying such files onto shared network drives, saving them on your Home Area (Office 365) and running them from your USB memory stick.

Staff and students are strictly forbidden from introducing music and video files (e.g. '.mp3, .mp4, .mpeg, .wav, .avi'). These files in many cases are copyrighted and the copying onto shared network drives or storing on your Home Drive (Office 365) may breach their copyright. Staff and students are strictly forbidden from downloading executable, music and video files when using the Trust's Internet provision.

16. Bring Your Own Device (BYOD)

Staff and students choosing to connect their personal devices the schools wireless network accept that, where appropriate, they must comply with the requirements and terms of this policy and abide by ICT Acceptable Use Policy.

17. Accessing Remote Systems

Students are only permitted to access remote systems authorised by Expanse Learning.

18. Saving Your Work

Students/employees must not use external media (e.g. USB memory and external hard disks) as their primary storage repository as it is not possible to recover lost or corrupted files. Students/employees are advised to save all files to their OneDrive account where it is routinely backed up and easily accessed both onsite and remotely. Students/employees are advised to regularly save amendments to their files to minimise data loss if their service is interrupted.

19. Administrator accounts/permissions

Employees who are granted with Administrator permissions must ensure that they only use the Admin account when required i.e. installing software or hardware etc. During their normal daily duties, they must use a local/standard account. Under no circumstances should an Admin use an Admin account to browse the internet.

20. Retention

In the event of a student or staff member leaving Expanse Learning, their Office 365 accounts will be deactivated with immediate effect, and all access will be revoked on the day of their departure:

- Students accounts will be completely deleted from Office 365 at the end of the Academic year.
- Staff accounts will be completely deleted from Office 365 after 12 months of their departure

21. Monitoring and Filtering

Expanse Learning will work in partnership with Wigan Council to ensure that systems to protect pupils are reviewed and improved. If staff or students discover an unsuitable site, it must be reported to Shared Services.

Monitoring software is in use for back-up purposes and to protect the security and integrity of the group systems. This software is also used to prevent Internet misuse, for example, by blocking access to inappropriate sites or materials by using filtering software. Information recorded by the automated monitoring systems can be used to identify an individual user and show, for example, a website or document that a user has been viewing and the time spent browsing. Head of Shared Services will undertake regular review of the Internet activity logs to monitor system performance. Expanse

Learning will undertake reviews at the specific request of management or by Shared Services. This may include review of usage and investigation of incidents and will be managed in accordance with local procedures.

Expanse Learning also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Expanse Learning is committed to supporting any investigation sanctioned by a Channel Panel. Expanse Learning using advanced web filtering systems provided by Agilysis UK, Wigan councils IT main Network Contractor, monitor and filter any web traffic they may or may not trigger a PREVENT referral.

Expanse Learning also reserves the right to carry out detailed inspection of any IT equipment without notice, where inappropriate activity is suspected. SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

All Networks (including Routers and Firewalls) are managed centrally via Wigan Councils central Firewall Smoothwall Application and located behind a Draytek Router which has a WAN interface IP managed on Wigan Councils Firewall Rules (managed by Agilysis UK)

Agilysis UK monitor:

- usage of the group curriculum computers and network
- captures records of misuse and unacceptable behaviour, such as swearing, accessing inappropriate or filtered websites and explicit images and identifies the user involved
- covers all internet use, all software, staff laptops, all websites, email, use of chat, forums and other social networking sites
- All inappropriate use, misuse or abuse is reviewed by Shared Services who then decide on the action to be taken.

In addition to this Sophos, a secure endpoint anti-virus and encryption software, is installed on all organisation devices. This software is monitored by the Shared Services Team.

The group curriculum network is filtered through the Wigan Council filtering system.

The list below is not exhaustive but contains examples of unacceptable use of the schools IT.

Content	Explanatory notes – Content that:
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography, offensive, obscene or indecent content	displays sexual acts or explicit images
Piracy and copyright theft	includes illegal provision of copyrighted material
Self-Harm	promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	displays or promotes the use of physical force intended to hurt or kill
Data Protection	that infringes the privacy and data protection rights of individuals
Bullying	that is defamatory, threatening, harassing, offensive or abusive
System Security	that is known to be infected with a virus, worm, Trojan or any form of malicious software or code

22. Monitoring arrangements

This policy will be reviewed every 12 months but can be revised as needed. It will be approved by the governing board

Impact of non-compliance

Staff:	Disciplinary action
Student:	Suspension, Temporary Exclusion, Permanent Exclusion
Legislation/organisational:	Reputational damage, statutory and non-regulated compliance. ICO Fines
Compliance lead:	Shared Services (ICT)
Policy Reference:	ELGR-POL-ICT-001
Version:	5
Agreed policy location:	DatabridgeMIS and Company Webpage
Does the policy require Governor approval?	No

Approval

Prepared by	***Approved by***	***Counter Signatory***
Scott Roberts (Assoc. CIPD)	Tony Brown	Richard King
01/09/2021	01/09/2021	01/09/2021
Head of Shared Services	CEO	Director of Schools & Pre 16 Education

Version Control

Version	***Date***	***Revision***	***Review Date***
1	04/01/2019	First Issue	03/01/2020
2	04/02/2019	Transferred to the new policy template	22/05/2019
3	01/09/2019	Policy review and transfer to the 2019-20 policy template	31/08/2020
4	01/09/2020	Policy Review, updated technical data around Server and Firewall protection	31/08/2021
5	01/09/2021	Policy Reviewed	31/08/2022