IT Acceptable Use Policy

Expanse Learning Group

October 2024

Author:
Eddie Wong

Version:
8

This Policy was approved by:
Board of Directors on 18th October 2024

Date for Review:
October 2025

1. Scope

This policy applies to all staff and students at Expanse Learning.

2. Introduction

Expanse Learning recognizes the educational value of electronic services and their potential to support the curriculum. Every effort will be made to provide quality experiences for both students and teachers using these services. However, inappropriate and/or illegal use of any information service is strictly prohibited.

Students should not have access to harmful or inappropriate material through Expanse Learning's IT system. However, care will be taken to ensure that 'over-blocking' does not lead to unreasonable restrictions on online teaching and safeguarding. To qualify for network, internet, and email access, students must read, sign, and return the acceptable use agreement.

If British decency laws or the Computer Misuse Act 1990 are breached, students may be referred to authorities, including the police. The Computer Misuse Act 1990 identifies three specific offences:

- Unauthorised access to computer material (programs or data).
- Unauthorised access to a computer system with intent to commit or facilitate a serious crime.
- Unauthorised modification of computer material.

Please read this document carefully. Access to the computer system will only be permitted once the acceptable use agreement has been signed and returned. Violation of the provisions of this agreement will result in the denial of access to the network, internet, and email and may lead to disciplinary action.

3. Personal Responsibility

As a representative of Expanse Learning, you are responsible for reporting any misuse of the network to a staff member. Misuse includes, but is not limited to, messages that indicate or suggest pornography, unethical or illegal activities, racism, sexism, inappropriate language, or attempts to disrupt or hack the network.

4. Acceptable Use

IT resources must be used to support work, educational activities, and research in line with Expanse Learning's educational goals and objectives. You are personally responsible for complying with these guidelines whenever you use any IT resource. Use of other networks or computing resources must adhere to the rules applicable to those networks (e.g., during work placements or when using partner group systems).

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 IT is a privilege. Inappropriate use may result in this privilege being withdrawn. Students will discuss appropriate behaviour and use of IT facilities with staff. Staff have the authority to deny, revoke, or suspend usage based on inappropriate use.

6. Network Etiquette and Privacy

All users are expected to follow accepted rules of network etiquette, including:

- **Be Polite**: Do not send or encourage others to send abusive messages. Respect others' rights and beliefs.
- **Use Appropriate Language**: Remember that you represent Expanse Learning on a global public system. Avoid swearing, vulgarities, or inappropriate language. Illegal activities are strictly forbidden.
- **Privacy**: Do not reveal personal information, including home addresses or telephone numbers, about yourself or others.

- **Passwords**: Do not share your password with anyone. If you believe someone has obtained your password, contact your line manager/tutor immediately.
- **Email**: Email is not guaranteed to be private. Messages related to illegal activities may be reported to authorities.
- **Cite references**: Cite references for any facts you present. Plagiarism may result in formal action, including withdrawal from examinations or qualifications.
- **Disruptions**: Do not disrupt the use of network services by others.

7. Services

Expanse Learning makes no warranties of any kind, expressed or implied, for the network services provided. It will not be responsible for any damages suffered, including data loss due to delays, non-deliveries, mis-deliveries, or service interruptions. Use of any information obtained via the network is at your own risk. Expanse Learning is not responsible for the accuracy of the information obtained through its internet services.

8. Security

If you identify a security issue, notify your line manager/tutor immediately. Never demonstrate security problems to other students. Use the system only with your own username and password, which must not be shared. Anyone caught disclosing passwords may have access denied and face disciplinary action. Staff should use password-protected screensavers and log out and shut down computers at the end of the day to allow for updates. Passwords should be at least 8 characters long and include a combination of letters, numbers, and symbols.

9. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy equipment or data, including the uploading or creation of computer viruses or wilful damage to hardware. Vandalism may result in loss of access and disciplinary action.

10. Online Ordering systems

Students are forbidden from using the internet to order goods or services or subscribing to newsletters, catalogues, or other forms of correspondence online.

11. Electronic Mail

The sending or receiving of emails containing inappropriate content (e.g., pornography, unethical or illegal requests, racism, sexism, or offensive language) is strictly forbidden. Disciplinary action will be taken for any violations. Large volume emails (spamming) are also prohibited.

12. Non-Educational Online Activity

Students may not access non-educational games, media (e.g., YouTube), or chat services without specific consent from their tutor.

13. Microsoft Teams

Microsoft Teams is for educational purposes only. It must not be used for social reasons or general chat. Refer to the Online Teaching Policy for more information. Misuse of Microsoft Teams may result in disciplinary action. Additionally, Microsoft Teams is used by IT for remote support and communication related to technical assistance.

14. Internet Search Engines

Students must use search engines responsibly. Any breach of this policy, including removing safety filters, may result in disciplinary action.

15. Executable, Music and Video Files

Staff and students are prohibited from introducing executable files (e.g., .exe, .cmd, .bat) to the network, as they may contain harmful viruses. Music and video files (e.g., .mp3, .mp4) are generally not allowed due to copyright issues.

16. Bring Your Own Device (BYOD)

Staff and students connecting personal devices to the school's network must comply with this policy and the IT Acceptable Use Policy.

17. Remote access systems

Students may only access remote systems that have been authorized by Expanse Learning.

18. Saving Your Work

Students and employees must use OneDrive as their primary storage solution and should not rely on external media (e.g., USB drives) or other cloud services to avoid data loss. Files saved to OneDrive are regularly backed up and can be accessed both on-site and remotely.

19. Administrator accounts/permissions

Employees with administrator permissions must only use these accounts for tasks like installing software or hardware. During normal operations, they should use a standard account. Admin accounts must not be used for browsing the internet.

20. Office 365 Account Deactivation and Deletion

When a student or staff member leaves Expanse Learning, their Office 365 accounts will be deactivated immediately. Relevant staff members must proactively provide detailed information to the IT department to facilitate the process.

- Student accounts will be deleted at the end of the academic year.
- Staff accounts will be deleted 12 months after their departure.

21. Monitoring and Filtering

Expanse Learning collaborates with Wigan Council to ensure that systems protecting students are regularly reviewed and updated. Monitoring software is employed to track network activity, prevent misuse, and detect inappropriate behaviour, which may result in disciplinary action. Expanse Learning also adheres to the statutory duty under **Section 26 of the Counter Terrorism and Security Act 2015** (PREVENT), ensuring that any suspicious activity is appropriately monitored and filtered. This includes the potential for a PREVENT referral if necessary.
Expanse Learning reserves the right to inspect any IT equipment without prior notice when inappropriate activity is suspected. The Senior Leadership Team (SLT) will conduct regular checks to ensure that filtering methods are appropriate, effective, and reasonable.

All networks, including routers and firewalls, are centrally managed through Wigan Council's Smoothwall Firewall and are supported by a DrayTek Firewall Router with WAN interface IP, governed by Wigan Council's firewall rules and managed by Agilysys UK.

Agilysys UK monitoring:

- The usage of group curriculum computers and the network.
- Records of misuse or unacceptable behaviour, such as inappropriate language, accessing filtered or inappropriate websites, and viewing explicit images, while identifying the user involved.
- All internet usage, software, staff laptops, websites, email, chat, forums, and social networking sites.
- Incidents of misuse, which are reviewed by IT, with decisions made regarding further actions.

In addition, **Microsoft Defender**, a secure endpoint antivirus and encryption software, is installed on all organization devices. The IT Team monitors this software to ensure protection and compliance.
The group curriculum network is filtered through Wigan Council's filtering system to safeguard internet access and maintain a secure learning environment.

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	Engaging in activities that compromise systems, including the use of anonymous browsing tools, filter bypass tools, or accessing sites that host malicious content.
Pornography, offensive, obscene or indecent content	Displays sexual acts or explicit images
Piracy and copyright theft	Includes the illegal distribution or use 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	Any activity that infringes on the privacy and data protection rights of individuals, including unauthorized access, use, or sharing of personal or sensitive information
Bullying	That is defamatory, threatening, harassing, offensive or abusive
System Security	Operating or allowing systems that are known to be infected with viruses, worms, Trojans, or any other 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
Policy Reference:	ELGR-ITSM-POL-0001
Version:	8
Agreed policy location:	PeopleHR, company Intranet and Webpage
Review Schedule:	12 Months
Does the policy require Governor approval?	No

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
6	01/10/2022	Policy Reviewed	01/10/2023
7	20/10/2023	Updated	19/10/2024
8	18/10/2024	Updated	17/10/2025