IT Acceptable Use Policy

Location	Oxford Campus, C/o Activate Learning, Jericho Building, Oxford OX1 1SA
Monitoring	The Principal and the management team EMN UK
Created by	Birgit Muller, Office Manager
Overall responsibility	Board of Directors
Created	July 2025
Last review date	na
Next review date	August 2026

1 Purpose

The purpose of this IT Acceptable Use Policy is to outline the acceptable use of all IT resources, including computer hardware and software, network systems, internet access, e-mail systems, and other electronic communication systems, by students, employees, contractors, and third-party service providers or visitors of EM Normandie UK Limited (hereafter 'EMN', 'EMN UK', 'the school', 'we', 'us').

EM Normandie acknowledges the positive effect which the use of Information Technology can have on achieving the highest standards of learning, teaching, innovation and research. Nevertheless, not all use made of IT is positive, ethical and legal and a framework is therefore required to regulate the use of the technologies and facilities made available by EM Normandie UK.

This policy seeks to provide such a framework to protect the integrity, confidentiality, and availability of the school's IT resources, and to promote responsible and ethical behaviour by users.

2 Scope

All members of the EM Normandie community, such as members of staff, students, contractors, visitors, etc. and any other individual who may, from time to time, be a user of the school's facilities and/or its IT resources, including the use of personal devices which are using the schools staff, student or visitors' Wi-Fi. It covers the use of all EM Normandie group's digital resources, as well as any external digital resources accessible from the school: data, software, hardware, login details, domain names, internal or external third-party information systems (which are subject to their own regulations).

3 Conditions of use

All users must comply with all applicable laws, regulations and are bound by the provisions made by all EMN's policies, procedures and statements, in addition to those made in this 'IT Acceptable Use Policy'.

Policies are available online at www.em-normandie.co.uk or can be obtained on request from the main administration office, 2nd floor, Jericho Building, Oxpens Road, Oxford OX1 1SA, from the Principal or the Office Manager.

The 'IT Acceptable Use Policy' should be read, in particular, in conjunction with the

- Student Code of Conduct
- Staff Code of Conduct
- Student Disciplinary Procedure
- Staff Disciplinary Procedure
- Statement of Freedom of Speech
- Safeguarding Policy
- Prevent Policy
- Data Protection Policy

3.1 Prevent duty

EM Normandie has a statutory duty under 'Prevent', Section 26(1) of the Counter Terrorism and Security Act 2015, to prevent members of its community from being radicalised and drawn into terrorism. In order to comply with this duty, the school reserves the right to monitor or block access to material that might incite hate, extremism, radicalisation or violence.

3.2 Access information

Access to systems such as an e-mail account, individual workstations, the IT network and applications, is protected by traditional login details (username and password) and additional multi-factor authentication (MFA). MFA reinforces access security by requiring identity validation of users via a mobile authentication app or a code received via a mobile phone text message.

- Login details are strictly personal and must be kept confidential. They should be memorised by the individual user and must not be saved to the system or shared with others, whether internally or externally, and
- users must not delegate their access details and user rights to third parties.

UK

3.3 Additional security measures for the safeguarding of professional data

All users have a responsibility to ensure the safeguarding of professional data. In addition to the provisions made regarding access information, users must therefore lock any devices, whether personal or professional, containing professional information, in any circumstance where the device is left unattended, even for short periods, to prevent access to professional and potentially confidential information by unauthorised individuals.

Basic security measures such as the automatic shutdown of sessions are essential and must not be disactivated by users.

3.4 E-mailing

E-mail services are provided by EM Normandie to support its primary role of education, research and associated functions related to this role.

All users are responsible for their own actions and have a responsibility to ensure their use of these services is appropriate and proper. In addition to their compliance with company policies referred to above and any current legislation, they must, all times, ensure that they do not

- create or communicate content which brings could bring EM Normandie into disrepute
- create or communicated content that is illegal
- communicate to a third party, any confidential information or material regarding EM Normandie and its operations
- create or communicate any content that may infringe on copyrights, including intellectual property
- carry out any activity that corrupts or destroys other users' data or disrupts the work of other users
- allow access to unauthorised persons to the company's systems
- use the service in any other ways which may be harmful to EM Normandie.

<u>Recommendations for the use of e-mail services</u>

- be aware of 'phishing' e-mails or attachments which may be infected with viruses ! Phishing e-mails often appear to be from a known provider and invoke an important issue which needs urgent attention. They may lure the user to malicious websites
- use professional language and keep the content concise and relevant
- try to stick to one topic: several short messages are preferable
- make the subject line informative and relevant
- avoid frequent use of capital, bold or underlined letters and words, as these can be perceived as the equivalent to shouting during a conversation
- ensure that confidentiality is maintained
- check whether 'all' have to receive a copy of your reply
- limit the number of e-mails, many matters may be dealt with through conversations via phone, teams or in person
- delete unwanted messages and those which are no longer needed

3.5 Data storage

The 'Cloud Microsoft 365' platform has been selected by EM Normandie for data storage and management, due to its strong security and compliance features.

Users are strongly advised to use this platform for any professional data.

EM Normandie may, from time to time, amend its policy or issue specific guidance in relation to the storage of and access to, data, to comply with new or updated legislation or other security advice.

3.6 Access by the company to data stored by users

The company reserves the right to access professional data stored by employees on company-owned devices and systems for work purposes in cases where the employee is suspected of misconduct or gross misconduct or where the company has another legitimate business interest to do so.

Users should not store personal information on company owned devices or system and any personal information stored on the company owned devices and system should be clearly marked and be easily identifiable as such.

3.7 Monitoring

Automated Monitoring

System logs are used to ensure the integrity of the EM Normandie IT systems, detect hardware/software errors, and monitor access and activity.

Monitored data includes

- Software use (access, file changes/deletion)
- Network, email, and internet connections (anomalies, site access, file downloads)
- Telephone calls (to detect unusual volumes or faults)

General automatic monitoring may be conducted in compliance with legal rules and all user activities and communication may be subject to monitored.

Users can access logs relating to them upon request to the Principal who will liaise with the IT department in France.

Manual Monitoring Procedure

If anomalies are detected, manual checks may be conducted on all EM Normandie tools and services provided, including the checking of files on local drives, Cloud spaces, backups, and e-mails.

Personal files and/or messages (marked accordingly) may only be viewed in the user's presence or in the presence of a nominated representative.

3.8 Reporting

Users have a responsibility to report immediately to their line manager, the Principal of the school or IT support, any suspected, attempted or actual breach of security and any other action which could undermine or put at risk the security, integrity, functionality and continuity of the information systems, as well as any indication of malfunction or other unusual occurrences which give rise to concerns.

3.9 Installation of software and settings on company owned systems and devices

Users are not permitted to install any software or application on company owned systems or devices, or to change settings on company owned devices, unless they have obtained prior written permission from the school to do so.

4 Personal Use

Users are encouraged to use the school's IT facilities only in the context of their work, study or research. The school permits personal use of the schools information systems and equipment as a privilege, not a right, and only as long as personal use

- does not interfere with the member of staff's work nor the student's study
- does not contravene any of the school's policies
- is not excessive in its use of resources
- any personal data stored on company owned devices or systems is clearly identified as personal data
- the security installed on personal devices ensures the safety of the organisation's information systems

5 User responsibilities

5.1 Any unauthorised access, use, or disclosure of personal information is strictly prohibited.

5.2 Users must comply with any request made to them by members of staff in connection with the enforcement of this policy.

5.3 Users shall not use the IT facilities inappropriately. See 2.2 for the unacceptable use examples.

5.4 Unacceptable Use

It is not acceptable for the school's IT Systems or equipment to be used directly or indirectly by a user, for accessing and/or creating, manipulating, transmitting, downloading or storing of

- any offensive, obscene or indecent images, data or other material, or any data capable of being

- unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise the user or others
- any material which promotes terrorism or violent extremism, or which seeks to draw individuals into terrorism or violent extremism
- unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of EM Normandie, other than in the context and for the purpose of, data collection in relation to OfS , Hesa and UKVI compliance
- material which is intended to be used to harassment, bullying and/or victimisation
- material which promotes discrimination on the basis of race, gender, religion or belief disability, age or sexual orientation
- material with the intent to defraud or deceive
- material which advocates or promotes any unlawful act
- material that infringes on intellectual property rights or privacy rights, or that is in breach of a legal duty owed to another party
- any other material which has the potential to bring the school into disrepute

It is equally unacceptable for the school's IT Systems or equipment to be used directly or indirectly by a user, for

- intentionally wasting staff efforts or other the school's IT resources
- corrupting, altering or destroying another user's data without their consent
- Disrupting the work of other users or the correct functioning of the school's IT Systems or equipment
- commercial activities or work related activities which are not in relation to the school's business
- the installation of software and devices for data-interception, password-detection or similar software or devices
- deliberate unauthorised access to the school's IT systems (hacking)
- any attempt to undermine the security of the school's IT systems, including any unauthorised penetration testing or vulnerability scanning
- the installation of any software or hardware without prior written authorisation

Where school's networks are being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the EM Normandie networks.

5.5 Exemptions from Unacceptable Use

There may be instances where legitimate academic activities are carried out using the school's networks that could be considered unacceptable use as defined above. Where there is any doubt whether any such usage may be treated as and exemption, written approval must be sought from the school's Principal in writing prior for any such activities taking place.

6 Consequences of breach of this policy

Any breaches of this policy by a user who is a member of the EM Normandie community, will be dealt with in accordance with the company's staff or student disciplinary procedures.

Where necessary, the company may also disclose information to the police or other agencies, such as the local authority, the Disclosure and Barring Service, etc., or take legal action to recover costs.

The company reserves the right to restrict or terminate a user's right to use the school's IT systems and equipment at any time once it becomes aware of a possible breach of this policy, including as a preventative measure during the period between an allegation being made and an investigation into an allegation coming to a conclusion.

The company also reserves the right to withdraw or remove any material uploaded by that user in contravention of this Policy.

Annex – Control table

Version	**V1**	Name	Role	Date
Created by :		Birgit Muller	Office Manager	Aug 2025
			Miriam Schmidkonz	
Approved by :		Miriam Schmidkonz	Principal	Aug 2025
Version		Name	Role	Date
Reviewed by :				
Approved by :				
Version		Name	Role	Date
Reviewed by :				
Approved by :				