Fairfield School of Business

Acceptable Use of IT Facilities

Version:	**4.0 (September 2022)**
Category:	Policies - Safety, Security and Environment
Owner(s):	Executive Committee
Approved by:	The Board of Governors
Access:	**Public** – Anyone can view this document
Scope:	This policy applies to all staff (including contractors and volunteers), students and visitors at Fairfield School of Business (FSB)

Acceptable Use of IT Facilities Regulations

The following defines that which constitutes acceptable use of the FSB's IT facilities, which primarily includes its desktop computers, laptops, printing facilities and internal networks. It expands upon the Employee and Student Codes of Conduct and is to be followed by all staff members and students.

These regulations are non-contractual and may be amended from time to time to meet the operational needs of the School.

Where IT users should fail to observe these regulations, the consequences can potentially be severe for the employee and for the School. The School must therefore treat any actual, attempted or suspected breach of these regulations seriously and may take disciplinary action against anyone acting or attempting to act in breach of it; in the most serious cases such action may include dismissal without notice for gross misconduct or expulsion from a programme of study.

These regulations are split into two sections:

- **Section A** outlines procedures applicable to **all** users of FSB's IT facilities and Networks
- **Section B** is applicable to **employees only** and concern their use of the School's IT facilities in the course of their day-today work.

These regulations do not extend specifically the use of social media by students or staff, which are dealt with in the School's Social Media Policy, however there may be some overlapping of themes regarding communication over company networks. For the avoidance of doubt, where an action would breach the school's codes of conduct in a physical environment, it would most likely do so in an online one.

Nothing in these regulations is intended to inhibit in any way the academic freedom of FSB's staff and students to engage in legitimate research activities relating to curriculum delivery; any access to online subject matter which would usually be prohibited by these regulations may be permissible with authorisation sought in advance from senior academics and network administrators.

Contents

The following themes are covered:

Section A

Section B

SECTION A

1. Examples of Unacceptable Use of IT Facilities

1.1. The School will not tolerate any instances of students or employees:

i. using School IT facilities in such a way that causes financial, material or reputational harm the School and/or those affiliated with it, for example by:

- unauthorised sharing of sensitive, confidential or strategic information,
- unofficially publishing personal views and values as those of the School,
- intentionally or unintentionally exposing School systems to malware (such as computer viruses) or other electronic security threats,
- causing damage to hardware and IT equipment

ii. using IT facilities in any way that would constitute bullying, harassment and/or victimisation of a person (as set out in the School's Dignity Policy),

iii. viewing, creating, sharing or distributing unlawful material or messages such that may be construed as libellous, defamatory threatening or extremist in content, or material which advocates breaking the law or in any way breaches the School's Prevent Duty policies,

iv. viewing, creating, sharing or distributing material which would be considered "Not Safe for Work" (or "NSFW"); this refers mainly to material containing nudity, explicit sexual references, profanity, violence, and/or other potentially disturbing subject matter),

v. attempting to gain access to another employee's or student's IT user account in order to act on behalf of that person, whether with or without their consent,

vi. downloading or disseminating copyright materials without the permission of the copyright owner,

vii. downloading or playing computer games.

1.2. Students and employees should exercise discretion in sending humorous material or jokes to colleagues over School networks and are advised to refrain from doing so, as material which they find acceptable might be offensive to others, and that even if the intended recipient is not offended by the message, it may be forwarded on to a person who is, in which case the original sender may be held to account.

1.3. Employees should not send humorous material or jokes to external parties as these may be misunderstood or cause offence; this behaviour does not align with FSB's standards of professional conduct.

2. Rules Regarding Use of IT Hardware

2.1. The following relates to treatment of the School's IT hardware (including computers, laptops, phones/smartphones, display screens/projectors, printer copiers, etc).

i. No IT equipment may be moved without the consent of the IT Department (with the exception of small items such as desktop phones, conferencing hubs and cables), and in such circumstances the IT Department will carry out the move.

ii. Any item of equipment belonging to the School that plugs into a mains outlet must be PAT tested by a certified practitioner; if there is no evidence that an item has been PAT-tested, this should be brought to the attention of the IT Team (it@fairfield.ac).

iii. No equipment may be attached to the School's network without the consent of the IT Department and in such circumstance the IT Department will carry out the attachment

iv. No equipment may be modified without the consent of the IT Department and in such circumstance the modification will be made by the IT Department.

v. All School IT equipment must be treated with care and left in good working order. Any fault, loss or damage must be reported by an employee to their Line Manager, as well as the IT Department immediately.

vi. All equipment must be logged off correctly and powered down when not in use for long periods of time; employees must turn off their PC at the end of each working day.

vii. School-issued laptops, tablet computers and mobile phones must be kept secure when taken off site and never left unattended in a public place. Employees are required to take all reasonable measures to minimise the risk of loss or theft occurring to School equipment and data.

viii. It is mandatory that employees re-boot their computer daily to enable periodic system updates, including important security updates, to take effect.

3. User Accounts and Login Credentials

3.1. All students and employees will be assigned a personal IT user account with specific login credentials (i.e. username and password) shortly after starting with the School, which can be used to log on to any computer connected to the School's network. A person's IT user account is for their use only; employees and students should take all reasonable steps to prevent unauthorised use of their user account by anyone other than themselves.

3.2. Individuals will be held responsible for all actions undertaken on a system which has been logged onto with their username and password, regardless of whether those actions where their own.

i. User account passwords are to be kept confidential and must not be shared with anyone. Employees and students should refrain from writing their password down in a place where it could be seen by anyone else.

ii. A logged-in workstation should never be left unattended; employees and students should always log out of or lock their workstations when not working at them to prevent unauthorised use.

iii. Where any employee/student suspects their login details may have been compromised, they should immediately notify their Line Manager/Administration Officer, who will request the IT Department to change them.

iv. Employees gaining or attempting to gain unauthorised access to another employees user account in order to view or edit files they should not have access to, or present themselves as another staff member, will be subject to disciplinary action which may lead to summary dismissal for gross misconduct.

4. Data Protection and IT Security

4.1. Employees and students must take reasonable steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data.

4.2. Anyone who suspects their computer, or any other workstation, may be infected with malware (such as a computer virus) must report the matter to their line manager or course leader and comply with the directions of the IT Department. Failure to do so can jeopardise the security of the School's computer network and could result in data loss / damage to computer hardware and software.

4.3. All attempts to circumvent the School's IT Security protocols, either deliberately or otherwise will be investigated by the IT Department and appropriate action will be taken. Examples of such actions would include disabling network firewalls, use of proxy servers to browse restricted websites, installation of software via 'back-door' methods, disabling security software, etc. Depending on the severity, such acts may lead to immediate dismissal for gross misconduct or expulsion form a programme of study.

4.4. Email file attachments should not be opened unless they are received from a trusted source, i.e. from another known School, employee or student or student representative. If in doubt, recipients should forward the email to the IT Department for verification.

SECTION B: Applicable to Employees Only

5. Emails and Instant Messaging

5.1. FSB's email and other internal communications platforms are to be used only for legitimate business purposes. All written communications sent over School servers are recorded and archived and may be viewed by the School at any time. Employees should therefore be mindful of the following when sending emails or personal messages from their user account:

i. The tone of all communications made via email, IM or CRM should be appropriate and professional; messages should never be of a hostile nature, use rude, inappropriate or threatening language or contain profanities.

ii. Communications should be proof-read and spellchecked, particularly where they sent in an official capacity to external recipients; this is to prevent ambiguity or misinterpretation arising, whilst preserving standards of professionalism.

iii. Emails sent to external networks will display a School footer, employees should not add their own footers or signatures to outgoing emails.

iv. It is accepted that Instant Messages between colleagues may be of a less formal nature; employees should nonetheless use their discretion when considering what would be an acceptable tone to use over the School's IM platform.

v. The School does not permit the use of its email for unofficial and/or personal purposes, including social invitations, personal messages, jokes, chain letters or other private matters, although this may be permissible in exception circumstances and with a Line Manager's permission.

vi. Emails to customers, suppliers and other business contacts should only relate to business matters. Confidential or sensitive information relating to the School or its employees should not be transmitted via email unless done so in the course of business and with a Line Manager's approval; where there is any doubt about whether certain information should be disclosed, the School's Data Protection Officer should be consulted.

vii. Email messages should only be sent to those for whom they are particularly relevant; the sender should refrain from copying in long lists of people who are peripheral to or not involved in the matter under discussion.

viii. Further to (vii.); employees should be aware that, as an email thread develops, it may no longer be appropriate to copy in people originally included, as this may be a distraction to those no longer involved or potentially result in disclosure of information to the wrong person(s).

ix. All internal communications are presumed confidential, and a communication which is exclusively between School employees must not be forwarded to external recipients (including consultants) unless it has been marked as "approved for external distribution" and/or specific agreement has been sought and received from the most Senior Manager copied in to such e-mail.

x. Employees who receive any email or personal message that is not intended for them should immediately notify the sender of the error and delete the message from their inbox to preserve confidentiality.

xi. Where unusual circumstances require an employee to use a non-School email address, the employee must seek the approval of their Line Manager for such usage, forward all messages sent and received by their personal account to the Line Manager, promptly delete all copies their personal email account once access to their School email is restored.

xii. Employees should not knowingly attach to emails, any files which may contain a virus, malware or spyware as the School could be liable to the recipient for any loss suffered by them as a result.

xiii. Employees should take care that there is no infringement of copyright when adding attachments to emails.

5.2. Further to the above the School may from time to time update employees with additional guidance on email etiquette and formalities; employees will be expected to exemplify this guidance in their correspondence.

6. Access Rights and Permissions

6.1. The access permissions assigned to an employee's user account will allow them to view only files, folders and directories that are relevant to their field of work, as per the approval of their Line Manager. Similarly, employees' access credentials may extend their access to School databases and Client Relations Management (CRM) platforms and special email boxes; again, the extent of access will be determined by the conditions attached to that employee's user account.

i. Employees requiring access to School files, datasets, applications or mailboxes in order to fulfil a work function should first seek permission from their Line Manager before forwarding that permission to the IT Department to process the request.

ii. All requests to the IT Department should clear about the extent and type of access (i.e. editing rights/read-only, etc.) required.

iii. Employees must not attempt to circumvent access restrictions; to do so may be construed as gross misconduct and result in summary dismissal.

iv. Where new access permissions would potentially grant an employee access to data defined as ‘sensitive’, ‘personal’ or ‘special category’ information within the School’s Data Protection Policy, the IT Department may first query the request with the School’s Legal Counsel, who may consult with the appointed Data Protection Officer (DPO); in this instance the employee and their Line Manager may need to justify the request for access in relation to the work function.

v. Employees who no longer require access to certain folders, directories, databases, etc. should relinquish this access as soon as possible by contacting their Line Manager and forwarding a request to the IT department as soon as possible.

7. Use of Portable Data Devices

7.1. The following pertains to the security of any electronic School data which is physically separate from the School’s networks; this might be information on portable storage media such as USB memory sticks (pen drives), DVDs and external hard drives, or it on portable computing devices such as laptops, tablet computers or smartphones.

i. Employees must not use portable storage media to transfer files between School computers; this should be done using the network drives and/or Intranet.

ii. School data should be loaded onto portable storage media only in urgent and/or exceptional circumstances with permission sought in advance form a Line Manager; all files should be removed from the device immediately once they are no longer needed and returned to a location on the School’s network or deleted.

iii. Employees transporting a portable data device with School information on it, whether on or off of School premises, should ensure the device is securely in their possession at all times; the device must never be left unattended (e.g. plugged into a computer workstation or left in an unlocked draw).

iv. Files stored on a portable device should be password protected and/or encrypted.

v. In the event that a laptop or other portable data device has been lost or stolen, this must be reported immediately to the appropriate Line Manager and the IT department; the Data Protection Officer should also be informed about any sensitive School or personal data on the device and the implications the loss of this data may have.

vi. Employees who receive media from any unknown source must have it virus checked by the IT Department. Employees bringing in media from a home computer must get permission from the IT Department before doing so.

Loaning of Portable Computing Devices

7.2. All portable computing devices (including laptops, tablet computers and smartphones) as well as accessories for this equipment (e.g. charging and data cables, carry cases, portable speakers, etc.) loaned to employees by the School for remote working shall be subject to a signed User Agreement.

7.3. The User Agreement shall make the employee liable for ensuring that such devices are used appropriately and for their intended purpose.

7.4. The User Agreement will clearly set out the terms and conditions of use for loaned computing equipment; where an employee is found in breach of any part of this agreement they may be sanctioned under the School's disciplinary procedures.

7.5. Further to 7.4, employees may be liable for the cost or replacing lost or damaged equipment up to the current market value of those goods, where this occurs as a result of their own misuse or failure to safeguard the equipment.

7.6. The School's IT Services shall retain the capability to remotely wipe the memory of a portable device at any time, should the company become aware of a risk to personal or commercially sensitive data.

7.7. The IT Services shall additionally wipe the memory of a device once it has been returned at the end of a loan and remove all active user accounts; the employee loaning the device is responsible for ensuring they have saved any files or documents they need before returning the device, as these will be irretrievable.

7.8. The IT services shall have a record of such equipment that is out for loan at any given time with details of what equipment has been loaned to whom. This record will include details of any breaches of the user agreement.

7.9. Where a person leaves the employment of the School, they will return any loaned equipment immediately upon leaving. The HR team will liaise with IT services when an employee leaves to ensure any loaned equipment is accounted for. In the event this equipment is not returned, the IT Services will remotely wipe the hard drive and deactivate any registered company account; the company may dock the final salary payment of the employee to cover the current market value of any unreturned goods.

Where devices connect to data networks

7.10. Further to clauses 7.2 – 7.9; use of company devices which are contracted on external data networks will be monitored. Employees may be required to account for any surplus costs run up on these contracts where such costs are attributed to inappropriate use of the device (such as accruing excessive call or data charges). In this instance, employees may be personally liable for such costs.

7.11. Employees will be personally liable for such costs, where the School deems these where not necessary to the business and/or are attributable to personal use.

8. Use of School Software and Work Applications

8.1. Employees' workstations will be set up by the IT Department and must not be altered by the user. This setup will include installation of any specific programmes and applications required by the employee to perform their role.

i. Under no circumstances will employees be permitted to purchase or load any unauthorised software without approval from their Line Manager and the IT Department. If a specific application programme is necessary for an employee's work, then the School will consider its purchase, and where approved, the IT Department will manage the download and installation.

ii. Standard operating procedures must be followed at all times when using software. Where no procedures exist, employees should consult with the IT Department and follow any instructions given.

iii. All original Read-only Memory devises (ROMs) should be kept with the IT Department.

iv. It is illegal to make unauthorised copies of software or use third party applications without lawfully obtaining the proper licenses. Software and computer facilities issued by the School for employees' use are licensed to the School and are protected by copyright law. Employees must not make copies of or distribute software that has been copied nor should they attempt to use unlicensed software applications. Employees who breach this condition will be subject to disciplinary action which could result in dismissal without notice for gross misconduct. Furthermore, persons who are found to making unauthorised duplicates of copyrighted software may be personally liable to prosecution under copyright law.

9. Internet Browsing at Work

9.1. Employees should note that the School reserves the right to monitor employees' use of its internet facilities and maintains a record of individual user's internet histories. Line Managers will be able to request a report on an employee's online activities whilst at work on a School computer where they may have concerns about the amount of time an employee spends online and/or the web content viewed.

9.2. Employees may at any time be called upon to justify the amount of time which they have spent on the Internet, or on any specific Internet site, during working hours.

9.3. The following outlines that which constitutes acceptable use of School Internet access:

i. All School computers have Internet access which is provided for business purposes only; employees personal internet browsing, or correspondences should be conducted during designated breaks and preferably on their own personal devices.

Note: Whilst at work, employees are still required to comply with the general provisions in Section 1 of this Code, regardless of whether they are using their own personal devices.

ii. Under no circumstances may any employee download any files from the Internet; this should only be done by the IT Department and with the written consent of their Line Manager

iii. Anyone believed to have been viewing unsuitable content as defined in Section 1 - iv. will be subject to disciplinary action. Offences of this nature may be considered gross misconduct and lead to dismissal without notice.

Note: The School subscribes to *internet 'reputation engines' which prevent access to* websites material considered be unsuitable for the work environment; this includes (but is not limited to) NSFW materials, sites linked to criminal activity or hate speech, gaming and gambling sites

iv. Whilst 'reputation engines' are highly effective at blocking prohibited material there is no assurance that all NSFW results will be blocked from an internet search; if content is not filtered out this does not mean it is acceptable to the School and employees may be held to account for the web content they view during work hours and/or using School IT facilities.

v. Employees must not enter into any licence or contract terms via the Internet on behalf of the School, without the prior express consent from the School.

10. Working from Home and Hybrid Working

10.1. The School will not usually permit the connection of personal devises to networks which contain protected information; restricted access may be permitted at the discretion of line managers, the School's Data Protection Officer and the Head of IT.

10.2. Employees granted remote working will usually be allocated company laptop subject to the restrictions outlined in Section 7.

10.3. The School may additionally prohibit the transfer of its intellectual property onto employees' personal devices, where such intellectual property is not already in the public domain.

11. Review of these Regulations

11.1. Changes to these regulations will be reviewed annually. All changes will be approved by the School's Board of Governors.

Appendix: Legal Framework

The Computer Misuse Act 1990 protects personal data held by organisations from unauthorised access and modification). Unauthorised access to computer material. This refers to entering a computer system without permission (hacking) Unauthorised access to computer materials with intent to commit a further crime.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The Act is intended to

- makes data protection laws fit for the digital age in which an ever increasing amount of data is being processed
- empowers people to take control of their data
- supports UK businesses and organisations through the change
- ensures that the UK is prepared for the future after we have left the EU

The Counter-Terrorism and Security Act 2015 creates a general duty on the School when exercising its functions to have due regard to the need to prevent people from being drawn into terrorism having particular regard to the duty to secure freedom of speech imposed by section 43(1) of the Education (No. 2) Act 1986 when carrying out that duty.

The Protection from Harassment Act 1997 creates both civil and criminal offences for harassment and makes provision for protecting persons from harassment and similar conduct.

The Equality Act 2010 requires the School, in the exercise of its functions, to have due regard to the need to eliminate discrimination, harassment and victimisation; advance equality of opportunity; and foster good relations between different groups.

Version Tracking:

Version	Author / revisions by	Changes summary	Approved by	Date
1.0 – 2.3	Head of IT Quality Unit Executive Committee	Original version and subsequent updates.	Board of Governors	Sep 2016 Sep 2017 Sep 2018
3.0 – 3.1	Risk and Audit Manager Head of IT (Network Manager)	Expanded 'Acceptable Use' definitions; alignment with Prevent Duty and Data Protection requirements; division into two sections; document reformatted applied.	Board of Governors	September 2019
3.2	Head of IT Quality Unit	Annual review and update.	Board of Governors	October 2020
4.0	Quality Unit Legal Counsel Senior HR Advisor IT Services Manager	Review and update- expansion of Section 7 guidance on portable data devices, and legal framework (Appendix); new document formatting applied.	The Board of Governors	September 2022

Date of next review: September 2023