



Information Technology Policy

Policy agreed	February 2020
Policy reviewed	July 2026
Policy due for review	July 2027
Produced by	Vickie Hillier
Reviewed by	Tony Sutton
Club review dates	N/A

1. Introduction

1.1. The Fitmums and Friends IT Policy is in place to protect both the charity and its employees and volunteers when working with technology and communication systems.

All employees must sign and agree to this Policy before gaining access to any level of technical equipment or software owned by or related to Fitmums and Friends.

2. IT Competency

2.1. Fitmums and Friends is committed to providing employees with the necessary tools and resources to do their job role, this includes IT systems and equipment.

If you feel you don't know how to use supplied IT equipment, Fitmums and Friends and the central team will always assist.

If you require IT training or assistance in any way shape or form, it is the employee's responsibility to inform the central team.

3. IT Responsibilities

3.1. Employees have access to computers and technologies at work for use in connection with Fitmums and Friends' business. Employees who are discovered unreasonably using Fitmums and Friends' computers for personal and private purposes will be dealt with under Fitmums and Friends' disciplinary procedure.

3.2. Vandalism of, or otherwise intentionally interfering with, Fitmums and Friends' computers/network constitutes a gross misconduct offence and could render the employee liable to summary dismissal under Fitmums and Friends' disciplinary procedure.

3.3. Misuse of any Fitmums and Friends equipment by an employee that results in fire, damage or personal injury will not be the responsibility of Fitmums and Friends. The employee must use a common sense approach when storing, securing and maintaining the equipment.

3.4. Any employee, who has use of Fitmums and Friends technology or equipment must not:

- Neglect to secure the equipment. E.g. leaving it on show in your car, misplacing it on a train.
- Leave the equipment in any extreme temperatures. E.g. keeping in a garage during winter or covering the equipment so that it has insufficient ventilation.
- Subject the equipment to accidental liquid spillages, submersion or show undue care or attention.
- Subject the equipment to damage from misuse or from showing undue care or attention.
- Lose possession, lend, sell or give away the equipment.

3.5. Any cases of misuse will be reviewed by the central team, and if deemed unacceptable, reported back to line management. All cases of misuse may result in a cost deductible from a persons' salary.

3.6. Where possible, the central team can supply employees with protective covers or protective cases depending on the nature of the job. The central team can also review staff requirements on an individual basis and can tailor your technology needs to your job specification.

3.7. At all times, any computer or piece of IT equipment issued to a member of staff is the property of Fitmums and Friends. The central team reserves the right to revoke, replace, or remove any issued equipment to staff. The employee does not have any specific ownership rights to an issued machine.

3.8. By agreeing to this policy, the employee agrees to take responsibility for these Fitmums and Friends owned assets and will make sure that they are well-cared for, kept in a safe environment and not misused.

3.9. Digital Security Responsibilities

Employees must follow Fitmums and Friends digital security standards including:

- Using strong passwords
- Using multi-factor authentication where provided
- Ensuring devices automatically lock when unattended
- Using only approved cloud systems such as OneDrive and SharePoint
- Not using personal email accounts for charity business
- Not sharing login credentials with any other person

These requirements support compliance with UK GDPR and charity cybersecurity obligations.

4. Damage, Loss, Theft or Misuse

4.1. Members of staff will have the use of computer equipment, either on a permanent basis or loaned temporarily. Such equipment is the property of Fitmums and Friends and must be looked after properly. In particular when equipment is being transported it must never be on show in the vehicle (i.e. always store equipment in the car's boot). If you are using the equipment at third party premises (e.g. at a club, at a college, etc.), you must not leave it unattended, unless the room is secured.

4.2. If Fitmums and Friends' IT property is lost or damaged, it will be replaced at Fitmums and Friends' expense the first time. If it is lost or damaged a second time Fitmums and Friends will replace it but will levy a charge for 50% of the cost from the employee. If the equipment is lost or damaged three or more times Fitmums and Friends will replace it each time but will levy a charge for 100% of the cost from the employee.

4.3. Any theft of computer equipment or telephones must be reported to the Police, and a crime reference number obtained. Theft or loss of equipment must also be reported to the individual's

line manager first. The central team will not issue replacement equipment until the line manager and/or Police have been notified.

4.4. All replaced equipment is not guaranteed to be new, and employees may be issued with refurbished models.

4.5. Reporting Data Loss

If any device loss or damage results in possible exposure of personal data, this must be reported immediately to the central team so Fitmums and Friends can assess whether the incident must be reported to the Information Commissioner's Office within 72 hours.

5. Faults

5.1. It is the employee's responsibility to report any faulty equipment belonging to Fitmums and Friends as soon as possible to the central team. If the equipment is deemed to be unsafe or in an unsatisfactory condition, it will be replaced by a reconditioned or new piece of equipment.

5.2. Report any of the following behaviour immediately:-

- The equipment is abnormally hot, or you smell burning whilst in use.
- The equipment begins to make a noise (Whirring or clicking).
- The equipment is tripping the electrical protection circuit (Similar to a power cut).
- You start to see unfamiliar errors not related to what you are doing.
- You notice that the screen cuts out or displays lines across it.
- Wires are exposed, or the chassis is damaged.
- You receive a static shock when in use.

5.3. It is imperative that faults are investigated as soon as they are recognised to protect employees and Fitmums and Friends.

5.4. Cybersecurity Incident Reporting

Employees must report any suspected cybersecurity incident immediately including:

- Phishing emails
- Suspicious links or attachments
- Ransomware warnings
- Unauthorised access attempts
- Unexpected password resets

Prompt reporting is required under UK GDPR and charity cybersecurity standards.

6. Computer software, games and viruses

6.1. Fitmums and Friends licences the use of computer software from a variety of outside companies. Fitmums and Friends does not own this software and, unless authorised by the software developer, neither Fitmums and Friends nor any of its employees have the right to

reproduce it. To do so constitutes an infringement of copyright. Contravention is both illegal and a disciplinary matter which will be dealt with in accordance with Fitmums and Friends' disciplinary procedure.

6.2. Only members of the central team have the authority to load new software onto any IT systems, equipment or device. Any employee found to be contravening this may face disciplinary action under Fitmums and Friends' disciplinary procedure.

6.3. Software and Cloud Application Controls

Only authorised members of the central team may install software, browser extensions, cloud applications or AI tools. Unauthorised installation may breach licensing laws, cybersecurity standards or GDPR.

7. Email and The Internet

7.1. Employees also have access to e-mail and the Internet for exclusive use in connection with Fitmums and Friends' business and as part of the normal execution of the employee's job duties. The purpose of these rules is to protect Fitmums and Friends' legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of confidential information.

7.2. Sending offensive, defamatory, malicious or otherwise unsuitable emails will not be tolerated, and any person doing so will be subject to Fitmums and Friends' disciplinary procedures.

7.3. E-mail should not be used for unsolicited correspondence or unapproved marketing campaigns and employees may not commit Fitmums and Friends financially by e-mail unless they have been granted a specific level of delegated authority to do so. Please note that these rules apply to all methods of communication (including, but not limited to: text messages, letters, memos, telephone calls, faxes and internet chat rooms).

7.4. Employees are permitted to surf the Internet for personal purposes during non-working hours.

7.5. Logging on to sexually explicit websites or the downloading and/or circulation of pornography or obscene material or using the Internet for gambling or illegal activities is prohibited, either during office hours, or in employees' own time. Any breaches of the policies above will be dealt with very seriously and could constitute gross misconduct and could render the employee liable to summary dismissal under Fitmums and Friends' disciplinary procedure.

7.6. Fitmums and Friends reserves the right to monitor employees' emails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

The purposes for such monitoring are:

- To promote productivity and efficiency.
- For security and legislative reasons.
- To ensure there is no unauthorised use of Fitmums and Friends' time e.g. that an employee has not been using e-mail to send or receive an excessive number of personal communications.
- To ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked
- To ensure that all employees are treated with respect, by discovering and eliminating any material that is capable of amounting to unlawful harassment.

7.7. If you receive an email in error, you must forward it onto the correct person and delete it from your system. If the email contains confidential information, use must not be made of this information, nor must it be disclosed.

7.8. Fitmums and Friends reserve the right to archive all emails, incoming and outgoing, despite deletion from the end user.

7.9. Fitmums and Friends reserves the right to deny or remove e-mail or Internet access to or from any employee physically from the admin page.

7.10. Monitoring Notice

Fitmums and Friends may monitor email, internet use and digital communications for legitimate business purposes including:

- Security and fraud prevention
- Ensuring compliance with policies
- Investigating misconduct
- Maintaining business continuity

Monitoring will be carried out in accordance with UK GDPR, the Data Protection Act 2018, the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act. Employees are informed that monitoring may occur and consent is implied through use of Fitmums and Friends systems.

7.11. Social Media and Messaging Apps

Employees must not use personal messaging apps such as WhatsApp, Facebook Messenger or SMS to store or transmit Fitmums and Friends data unless specifically authorised. All official communication must use approved systems to ensure GDPR compliance.

8. External USB Storage

8.1. USB storage, hard drives and the like may be used to transfer data between computers, if it is unfeasible to copy the data to the network, or to email it. However, all business data remains, at all times, the property of Fitmums and Friends.

8.2. If personal USB keys are used, then they must not install any software onto your computer. If you require a USB key, the central team has a central store of keys that can be loaned to employees temporarily.

8.3. Employees must not purchase or use donated USB memory sticks as this could introduce security issues due to viruses and other vulnerabilities. All external USB memory sticks must be virus scanned before use.

8.4. Once you have transferred data using a USB device, immediately delete it from the device.

8.5. Modern USB Restrictions

USB devices may only be used where absolutely necessary. Where possible employees must use secure cloud storage instead of USB devices. All USB devices must be encrypted and scanned before use.

9. Data and Content

9.1. All data generated by employees, or on behalf of Fitmums and Friends, remains at all times the intellectual property of Fitmums and Friends. This includes documents prepared by staff, contact details (e.g. customer contact details), emails and other electronic communication.

9.2. All digital content produced, distributed and owned by Fitmums and Friends must not be sold or reproduced. For example, game footage or images must not be distributed by an employee unless there has been express permission from the respective departments in charge of the content. If this is contravened, there is strong possibility Fitmums and Friends may be fined due to copyright infringements or break confidentiality agreements between sponsors and partners. This may result in disciplinary action and dismissal of the offending employee.

9.3. GDPR Compliance Statement

Fitmums and Friends processes personal data in accordance with UK GDPR and the Data Protection Act 2018. Employees must ensure data is stored securely, accessed only for legitimate business purposes, not retained longer than necessary, not shared outside authorised systems and that personal data breaches are reported immediately

9.4. Data Subject Rights

Employees must respect individuals' rights under UK GDPR including:

- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing

- Right to data portability

Requests must be forwarded to the central team immediately.

10. Leaving the company

10.1. If you are leaving Fitmums and Friends, you will need to do the following prior to your leaving date:-

- Arrange with the central team a suitable technology handover plan, where you can work out who you need to pass the company data you hold onto, and what you are going to do with your emails in the transition period.
- Ensure that all personal data is removed from all Fitmums and Friends Devices, these will be wiped a week after your leaving date and will be non-retrievable.
- Arrange with the central team a date and time where you can return all equipment and have it checked off.

10.2. Fitmums and Friends reserves the right to protect intellectual data and company property, therefore on leaving the company you must not:-

- Retain company data, contacts or emails.
- Forward company data to another email address or persons for personal gain.
- Use company data to approach customers, clients or other associates that will conflict the interests of Fitmums and Friends.

10.3. Breach of information from leavers may result in Fitmums and Friends seeking legal advice.

10.4. Fitmums and Friends reserves the right to recoup costs of damaged equipment on their return.

10.5. GDPR Exit Requirements

Upon leaving Fitmums and Friends:

- All access to systems will be revoked on the leaving date
- Emails and digital content may be retained for lawful business purposes
- Personal data stored on devices will be securely wiped in line with GDPR retention rules
- Leavers must not retain or transfer any Fitmums and Friends data

11. Equality, Accessibility and Reasonable Adjustments

Fitmums and Friends will provide reasonable adjustments under the Equality Act 2010 for employees who require support using IT systems. This may include assistive technology, alternative formats, modified equipment or additional training. Employees should inform the central team if adjustments are required.

12. Cybersecurity and Incident Response

Employees must report incidents immediately, follow instructions from the central team, cooperate with investigations and avoid attempting to fix security issues themselves. This ensures compliance with UK GDPR and charity cybersecurity standards.

Signature sheet – IT Policy

Volunteers with laptops and paid members of staff must be supplied with a copy of the IT Policy and should sign this document to say this has been shared and discussed with them.

Please sign below to confirm that you have read and understood this Fitmums and Friends IT Policy.

Name: _____

Role in Club: _____

Signed: _____

Date: _____

Counter signature (Club Co-ordinator/Trustee/Central Team)

Signed: _____

Print Name: _____

Role: _____

Date: _____

For office use:

X1 copy scanned & emailed to admin@fitmums.org.uk

X1 copy for individual

