IT Acceptable Use Policy

Trust Staff Version

DISTRIBUTION	This is a Trust-wide policy and applies to all staff within the Trust.		
DOCUMENT ID	FT-IT001 Acceptable Use Policy (Staff)		
AUTHOR	HRS	**VERSION**	3.1
RATIFIED BY THE DIRECTORS OF THE FALLIBROOME TRUST			
POLICY REVIEW CYCLE		3 YEARS	
POLICY REQUIREMENT		NON-STATUTORY	

The Fallibroome Trust, Priory Lane, Macclesfield, Cheshire, SK10 4AF
Telephone: +44 (0) 1625 827 898 | Email: info@fallibroometrust.org.uk | Web: www.fallibroometrust.org.uk

CONTENTS

INTRODUCTION

This Acceptable Use Policy (AUP) policy is applicable to all Fallibroome Trust staff, both teaching and non-teaching. It applies when staff are working in their usual place of work and when staff are working remotely or travelling.

CONTEXT

IT is an integral part of all modern business settings and is essential within the context of educational settings. The purpose of the policy is to recognise the need for all staff to be able to utilise the Trusts IT systems for the legitimate purposes for which they need it in order to carry out their professional duties.

This policy reflects the Fallibroome Trusts broad principles in relation to acceptable use of IT and IT security. It will be subject to further revisions and will be developed so that a suite of documentation is available relating to eSafety and data protection (including individual acceptable use statements signed by staff and by students/parents).

All staff are expected to comply fully with this policy. The Fallibroome Trust reserves the right to take disciplinary action in the event that it considers that a member of staff is acting in contravention of this policy. In addition, and in any event the Fallibroome Trust reserves the right to consider legal proceedings against any member of staff who breaches this policy.

SUPPORTING DOCUMENTS

This policy is supported by several other Fallibroome Trust policies or guidelines, notably:

- FT-IT004 - eSafety policy
- FT-IT005 - Data Protection - Main Policy
- FT-IT007 - Data Protection - Data Encryption Policy
- FT-IT009 - Data Protection – Student Image Consent
- FT-IT010 - Privacy Notice - Staff (including Consultants and Volunteers)
- Safeguarding Young People / Staff Code of Practice
- Staff Disciplinary policy
- Anti-Bullying and Child Protection policies

ADVICE AND GUIDANCE

If you have any concerns, or would like further advice and guidance at any time relating to this policy please contact the Trust Chief Information Officer, local IT Support Team or the designated leader for Child Protection for matters relating to the Safeguarding of Children.

THE LAW

Several laws are relevant to the use of IT services and therefore we are obliged to operate within them. Some conditions within this AUP are requirements in law, in brief the relevant (but not limited to) laws include:

- **Computer Misuse Act:** This covers the unauthorised access to data, devices or systems and any resulting criminal activity
- **Copyright, Design and Patents Act:** This covers the copying or downloading of software, documentation, or other intellectual property
- **Data Protection Act:** This covers the use, disclosure, and storage of personal data. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR)
- **Regulation of Investigatory Powers Act:** This covers guidelines for the monitoring of user activities on both internal (The Fallibroome Trust) and external IT systems
- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations:** This covers the lawful monitoring of communications systems
- **The Human Rights Act:** People's rights and responsibilities are properly balanced and where an awareness of the Convention rights permeates our government and legal systems at all levels

IT staff who are specifically authorised by the Fallibroome Trust to do so may monitor and inspect any aspect of use of academy or Trust IT equipment/systems, without prior notice, to the extent permitted by law.

NOTE: If there is an incident that is considered a breach under the Data Protection Act this may require investigation by the Information Commissioner's Office and heavy financial or other sanctions could apply to the Fallibroome Trust.

THE ACCEPTABLE USE POLICY

This AUP covers the use of all the IT systems, owned or operated by The Fallibroome Trust. As stated previously it applies to activities on premise, at home or any other location where The Fallibroome Trust IT systems are accessed.

THE FALLIBROOME TRUST IS RESPONSIBLE FOR

- A safe and secure network environment available to all staff in The Fallibroome Trust
- Advanced web and email filtering systems to protect staff from offensive content
- A secure eSafety policy to deal with any suspected incidents or breaches
- Secure access to any remotely available IT systems whilst not on the premises
- An eLearning environment to support student learning
- Effective monitoring procedures
- Adherence to the legal framework
- Advice and guidance for all staff
- A regular review of services and security

CONDITIONS OF THE ACCEPTABLE USE POLICY

- All staff must take responsibility for reading and upholding the standards laid out in the AUP
- All staff should understand that the AUP is under annual review and can be amended at any time
- All staff must take responsibility for their own use of technology, making sure that they use IT resources safely, responsibly, and legally
- All staff must be active participants in eSafety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies
- No applications or services accessed by staff may be used to bring The Fallibroome Trust, or its members, into disrepute
- No communications device, whether provided by The Fallibroome Trust or personally owned, may be used for the bullying or harassment of others in any form

- All staff have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others

- All staff have a responsibility to ensure the safety and security of sensitive and personal data, including the transferring of data between systems and locations using removable media. In addition files and media should be encrypted (see FT-IT007 - Data Protection - Data Encryption Policy)

- All staff have a responsibility to report the loss of data or equipment to the IT Department as soon as possible

- Staff are not permitted to pass personal information about other people (e.g. name, phone number, email address) to other organisations without the relevant authorisation

- All staff have a duty to respect the technical safeguards that are in place. Any attempt to breach technical safeguards, or gain unauthorised access to systems and services, is unlawful and may result in disciplinary action

- All staff have a duty to report failings in technical safeguards which may become apparent when using the systems and services

- All staff have a duty to protect their passwords and personal login details, and should log off the network or device when leaving computers/devices unattended or as a minimum "lock" the device

- Any attempts to access, corrupt or destroy other staff data, or compromise the privacy of others in any way, using any technology, is unlawful and may result in disciplinary action

- All staff members should ensure that students comply with The Fallibroome Trust IT Acceptable Use Policy for Students and that appropriate sanctions are issued if this policy is breached

- All staff should use the IT facilities sensibly, professionally, lawfully, in a manner consistent with their duties and with respect for pupils and colleagues

- All staff must respect the copyright and intellectual property rights of third parties

Staff should be aware that:

- Network activity and online communications may be monitored, including any personal communications made via The Fallibroome Trust network and systems

- Under certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

- Once information is shared online it is completely out of the control of The Fallibroome Trust and may be used by others in a way that was not intended

- If an incident occurs that is considered to be an offence under the Computer Misuse Act, Data Protection Act it may require investigation by the police and could be recorded on any future criminal record checks

PHOTOGRAPHS AND DIGITAL MEDIA

- Written permission from parents or carers will be checked / obtained before photographs of pupils are taken (see FT-IT009 – Data Protection – Student Image Consent) for use
- Student work may only be published with the written permission of a parent/guardian and the student on public systems such as The Fallibroome Trust website or Trust school website
- Photographs of students must be carefully selected and appropriate for context
- Students full names should not normally be used to identify individuals in a photograph, see the media release letter for exceptions
- Staff must use The Fallibroome Trust cameras to photograph students. Staff must not use personal equipment without authorisation from the Principal/ Head of School/ Head teacher or Executive Principal
- Storage cards and media should be cleared when the camera is returned
- Photographs of students should only be stored in a secure area within the school's relevant network areas
- When photographs are taken whilst off site (e.g. school trips) the images should be put onto The Fallibroome Trust systems as soon as is practicable
- Photographs of students must be deleted when no longer required

USING STAFF MOBILE DEVICES:

- Staff may be supplied with Fallibroome Trust equipment to utilise at home and outside of their usual work place setting. Such equipment must be treated and used in the same way, as it would in the workplace.
- On request, staff must make portable and mobile IT equipment available for antivirus updates and software installations, patches or upgrades. The installation of any applications or software packages must be authorised by the Trust, fully licensed and only carried out by the Trusts IT team.
- Staff are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.
- IT equipment must not be left unattended in an area accessed by the public and/or when travelling. When travelling by car, if a staff member must leave the car unattended then IT equipment should be kept locked in the boot and out of sight.

ELECTRONIC COMMUNICATION WITH STUDENTS OR PARENTS

Private communication with students of a personal nature is inappropriate (see the staff code of practice):

- Students should not be listed as approved contacts on any social networking sites
- Staff should not use or access the social networking sites of pupils
- Staff should not give out personal contact details to students, including mobile phone numbers, unless in exceptional circumstances agreed in advance with the Principal/ Head of School/ Head teacher or Executive Principal
- Staff should only give permission to pupils to communicate online with trusted sources

Where electronic communication is necessary, members of staff must:

- Only use The Fallibroome Trust approved email and phone systems to contact students and parents
- Avoid using personal mobile phones and other handheld communication devices for communication with students or parents