IT and Internet Acceptable Use Policy

Document Control

Date	Revision amendment details	By whom
Feb 2019	Adopted by TEFAT Board	Trustees
Feb 2022	Statutory updates and required revisions reviewed and approved	Ops Group
March 2022	Adopted by TEFAT Board	Trustees
Feb 2024	Reviewed in line with RM support on Cyber Security Essentials Compliance	Ops Group
March 2024	Adopted by TEFAT Board	Trustees
March 2027	Proposed date for review subject to any required statutory update	Ops Group

Table of contents

Elliot Foundation Academies Trust Values 3

Related policies and documents 4

Definitions 4

Policy statement and objectives 5

Scope and principles 5

Trust's responsibility 5

User responsibility 5

Digital Identity 5

Reputation 5

Access 5

Misuse of technology 6

Explicit acceptance of active and passive monitoring 6

Compliance with related policies 6

Elliot Foundation

Elliot Foundation Academies Trust Values

1. Put children first

a. We trust and value your professionalism
b. We share the responsibility for the learning and welfare of all of our children
c. Our purpose is to improve the lives of children

2. Be safe

a. Don't assume that someone else will do it
b. Look after yourself, your colleagues and all children
c. We are all responsible for each other's safety and well being
d. Discuss any concerns with an appropriate member of staff

3. Be kind & respect all

a. People are allowed to be different as are you
b. Kindness creates the positive environment we all need to flourish
c. This kindness should extend to ourselves as well as to others

4. Be open

a. If you can see a better way, suggest it
b. If someone else suggests a better way to you, consider it
c. We exist to nurture innovators and support those who take informed risks in the interests of children

5. Forgive

a. We all make mistakes
b. Admit them, learn from them and move on

6. Make a difference

a. Making the world a better place starts with you
b. Model the behaviour that you would like to see from others

Related policies, documents & legislation

- User’s place of work Acceptable Use Policy
- TEFAT Bullying and Harassment Policy
- The Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- The Protection of Children Act 1978

Definitions

- Where the word 'Trust' is used in this document it refers to The Elliot Foundation Academies Trust.

1. Policy statement and objectives

1.1. Today’s schools cannot function without the internet, mobile devices and computers. But ubiquitous technology brings significant additional risks. The purpose of this policy is to keep all children and staff safe in the simplest terms possible.

2. Scope and principles

2.1. This policy applies to all employees of the Elliot Foundation, those with a responsibility for governance, service providers and contractors to the Trust and any other volunteers who access Trust electronic systems or devices.

3. Trust responsibility

3.1. The Trust will provide and maintain an IT network and internet connectivity of an acceptable standard with hardware and software controls to mitigate risks where possible.

4. User responsibility

4.1. Users accept responsibility for their own digital actions.

4.2. Users accept that Trust systems may only be used for purpose in line with Trust values

5. Digital Identity

5.1. Users must only access Trust networks, devices and services with their Trust provided digital identity (email and password).

5.2. Users must take reasonable steps to protect the security of their digital identity including but not limited to:

- 5.2.1. Changing their password to a new password that is in keeping with Trust Password Protocol on first receiving any new Trust email account
- 5.2.2. Avoiding using the same password for Trust accounts that are also used elsewhere for personal accounts
- 5.2.3. Ensuring their password is not written down
- 5.2.4. Recording their password electronically only in encrypted and secure password safes
- 5.2.5. Using TEFAT approved Multi Factor Authentication where possible

5.3. Users may not share their passwords with any other person.

6. Reputation

6.1. No applications or services accessed by users as part of their employment or using Trust infrastructure or devices may be used to bring the school, the Trust, its children or staff into disrepute.

7. Access

7.1. All users must respect technical safeguards which are in place (e.g. RM Unify). Any attempt to breach technical safeguards, conceal network identities, use jail-broken devices, ignore security updates or gain unauthorised access to systems and services is unacceptable and may be treated as a disciplinary offence.

8. Misuse of technology

8.1. No Trust device, network or platform may be used to harm others or break the law (this includes cyberbullying, hacking, illegal file sharing, trolling etc).

8.2. Failure to comply with this policy may be treated as a disciplinary offence.

9. Explicit acceptance of active and passive monitoring

9.1. All users accept that the Trust will conduct active and passive monitoring of all systems, devices and digital communications using its networks in order to keep users safe and to comply with the laws of the land.

10. Compliance with related policies

10.1. All users accept responsibility for informing themselves of the latest version of central and local related policies listed above and complying with their terms.

11. Physical security and secure disposal of IT equipment

11.1. Staff must take reasonable care of their Trust issued IT equipment and are responsible for ensuring its physical security

11.2. All Trust provided IT equipment must be returned to the IT support team for secure disposal

12. When in doubt seek help

12.1. Technology can be daunting. If you have any concerns or problems, don’t assume that everything will be ok, report them to tefatsupport@rm.com

12.2. If you see anyone acting suspiciously on or around Trust IT systems report them immediately to your school principal or line manager