E-Safety Policy

Date created: November 2025

Created by: Mr P Marsden

Review by: November 2026

1. Introduction

This policy sets out the approach of Active Futures Academy to ensuring the safe and responsible use of digital technologies, the internet, and online platforms by learners, staff, and visitors.

Our provision recognises that digital technologies are an essential part of everyday life, learning, and social interaction. However, they also present risks. We are committed to safeguarding learners by promoting safe, responsible, and respectful use of technology.

This policy should be read alongside:

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Data Protection Policy

2. Aims and Objectives

The aims of this policy are to:

- Protect learners from online harm, including grooming, exploitation, radicalisation, cyberbullying, and exposure to inappropriate content.
- Educate learners to use technology safely, critically, and respectfully.
- Support staff to model safe online behaviour and respond effectively to concerns.
- Ensure systems are in place to monitor, filter, and manage digital technology use.
- Fulfil statutory safeguarding responsibilities in line with *Keeping Children Safe in Education* (KCSIE).

3. Scope

This policy applies to:

- All learners enrolled at the Active Futures Academy.
- All staff, contractors, and volunteers.
- Parents/carers supporting learners’ online engagement.
- All devices and platforms used for learning and communication, including personal devices when accessing AEP networks.

4. Roles and Responsibilities

Directors / Senior Management

- Ensure appropriate monitoring, filtering, and safeguarding measures are in place.
- Review and approve this policy annually.

Designated Safeguarding Lead (DSL)

- Act as the central point of contact for online safety concerns.
- Keep up to date with national guidance and training.
- Record and respond to online safety incidents in line with safeguarding procedures.

Staff

- Model safe, responsible, and professional online behaviour.
- Embed e-safety education into curriculum delivery.
- Report concerns immediately to the DSL.

Students

- Use technology responsibly, following the Active Future's Acceptable Use Agreement.
- Report any online concerns, bullying, or unsafe activity to staff.

Parents/Carers

- Support safe use of technology at home.
- Engage with the Active Future's e-safety guidance and resources.

5. Education and Training

- **Learners** receive regular sessions on online safety, tailored to their age, ability, and additional needs, covering topics such as:
  - Online privacy and security.
  - Cyberbullying and respectful communication.
  - Recognising online grooming and exploitation.
  - Managing online reputation and digital footprint.
  - Critical thinking about online information (misinformation, extremism).
- **Staff** undertake annual training on online safety, including emerging risks, in line with safeguarding responsibilities.
- **Parents/carers** are provided with guidance on supporting online safety at home.

6. Filtering, Monitoring, and Security

- Active Futures Academy provides secure internet access with appropriate filtering to protect against harmful content, while enabling educational research.
- Network activity is monitored to identify misuse or safeguarding concerns.
- Personal devices may only be used in line with the Acceptable Use Agreement and under staff supervision.
- All devices are protected with antivirus software and regular updates.
- Data is managed securely in line with GDPR.

7. Responding to Incidents

- Any online safety concern will be treated as a safeguarding issue and reported to the DSL.
- Concerns will be logged and managed in line with the Safeguarding & Child Protection Policy.
- Where necessary, the Active Futures Academy will liaise with external agencies such as CEOP, the police, or social care.
- Sanctions for misuse will follow the Behaviour Policy.
- Support will be provided to any learner affected by online harm.

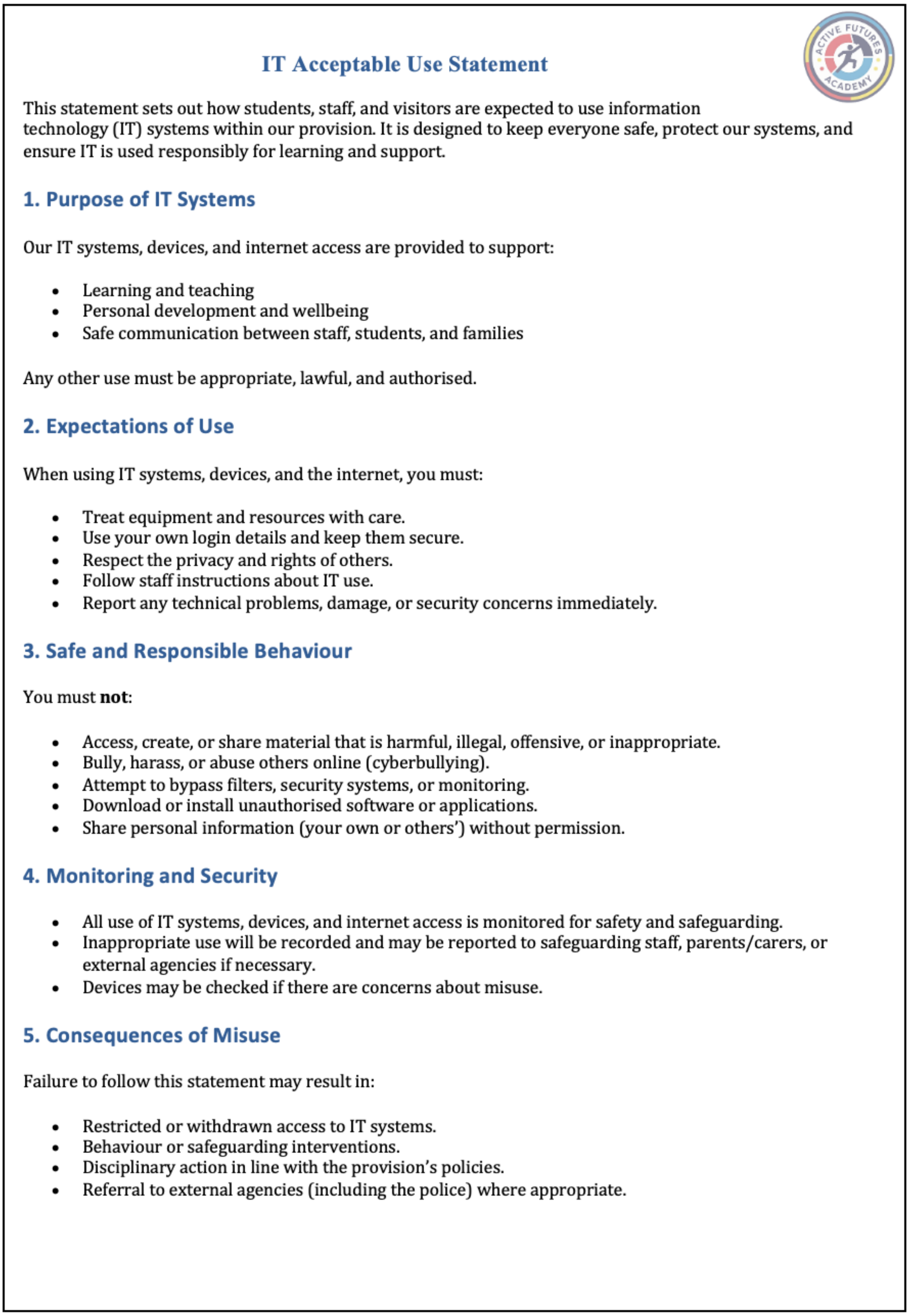
8. Prevent Duty

We recognise our duty under the *Counter-Terrorism and Security Act 2015* to prevent learners from being drawn into terrorism. Staff are alert to online radicalisation risks and learners are taught to critically evaluate extremist content online.

9. Policy Review

This policy will be reviewed annually by the DSL and management committee, or sooner if significant developments in technology, statutory guidance, or safeguarding practice occur.

Appendix A – IT Acceptable Use Policy



IT Acceptable Use Statement

This statement sets out how students, staff, and visitors are expected to use information technology (IT) systems within our provision. It is designed to keep everyone safe, protect our systems, and ensure IT is used responsibly for learning and support.

1. Purpose of IT Systems

Our IT systems, devices, and internet access are provided to support:

- Learning and teaching
- Personal development and wellbeing
- Safe communication between staff, students, and families

Any other use must be appropriate, lawful, and authorised.

2. Expectations of Use

When using IT systems, devices, and the internet, you must:

- Treat equipment and resources with care.
- Use your own login details and keep them secure.
- Respect the privacy and rights of others.
- Follow staff instructions about IT use.
- Report any technical problems, damage, or security concerns immediately.

3. Safe and Responsible Behaviour

You must **not**:

- Access, create, or share material that is harmful, illegal, offensive, or inappropriate.
- Bully, harass, or abuse others online (cyberbullying).
- Attempt to bypass filters, security systems, or monitoring.
- Download or install unauthorised software or applications.
- Share personal information (your own or others') without permission.

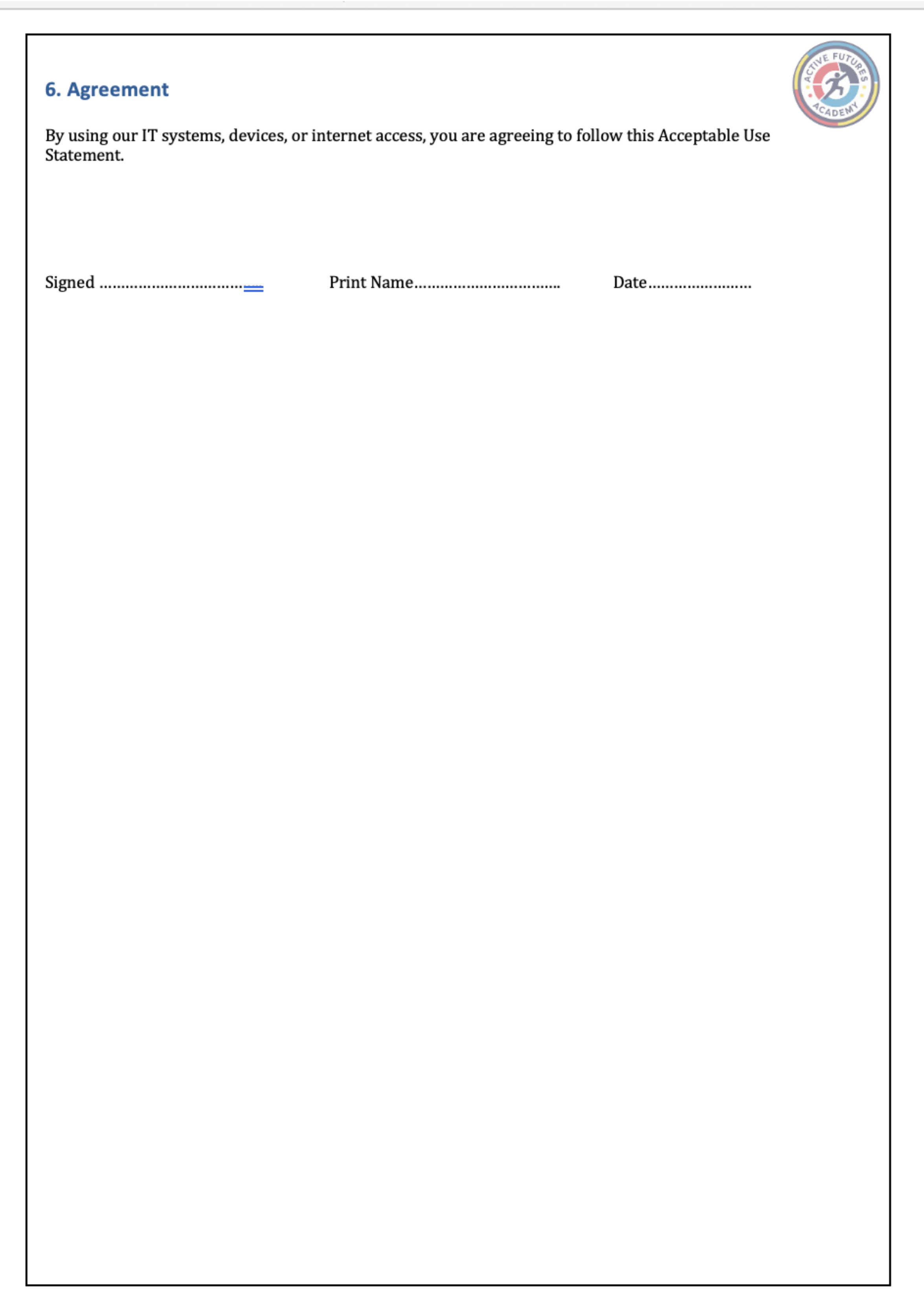
4. Monitoring and Security

- All use of IT systems, devices, and internet access is monitored for safety and safeguarding.
- Inappropriate use will be recorded and may be reported to safeguarding staff, parents/carers, or external agencies if necessary.
- Devices may be checked if there are concerns about misuse.

5. Consequences of Misuse

Failure to follow this statement may result in:

- Restricted or withdrawn access to IT systems.
- Behaviour or safeguarding interventions.
- Disciplinary action in line with the provision's policies.
- Referral to external agencies (including the police) where appropriate.



6. Agreement

By using our IT systems, devices, or internet access, you are agreeing to follow this Acceptable Use Statement.

Signed .... Print Name................................. Date........................