StudyBox Acceptable Use Policy (AUP)

(Aligned with Keeping Children Safe in Education 2025)

1. Purpose and Scope

This Acceptable Use Policy (AUP) sets out the expectations for safe, responsible, and respectful use of technology at StudyBox. It applies to all children and young people attending StudyBox, and to all staff, tutors, volunteers and visitors who use StudyBox devices, systems, or internet access.

The policy aims to:
- Protect children and young people from online harm.
- Promote safe and responsible digital behaviour.
- Support compliance with Keeping Children Safe in Education (KCSIE) 2025 and the Data Protection Act 2018 (GDPR).
- Protect the integrity and security of StudyBox's IT systems and data.

2. General Principles

- The use of StudyBox digital systems, internet access, and devices must always support learning and wellbeing.
- All users must act in accordance with StudyBox's Safeguarding Policy, Code of Conduct, and Data Protection Policy.
- Access to systems and devices is a privilege, not a right; it may be restricted or withdrawn if misused.
- Inappropriate use may result in safeguarding action, loss of access, or disciplinary procedures.

3. Responsibilities

a. Staff, Tutors, and Volunteers

All adults working with children at StudyBox must:
- Use IT systems, the internet, and email only for professional purposes.
- Keep passwords secure and never share login credentials.
- Use StudyBox email accounts for all work-related communications.
- Never communicate with pupils through personal devices, email, or social media.
- Avoid accessing or storing illegal, extremist, or inappropriate content.
- Report any accidental access to such content immediately to the Designated Safeguarding Officer (DSO).
- Ensure that any personal data or pupil information is stored and transmitted securely.
- Use only approved devices and platforms for remote learning or online sessions.
- Immediately report any safeguarding concerns, online incidents, or data breaches to the DSO.

Online Conduct:
- Staff must maintain clear professional boundaries online at all times.
- Staff should not "friend," "follow," or message pupils or their family members on social media.
- Personal opinions shared online must not compromise StudyBox's reputation or professionalism.

b. Pupils and Young People

All children and young people attending StudyBox must:
- Use computers, tablets, and the internet for learning purposes only.
- Treat others with respect online — no bullying, harassment, or sharing of harmful material.
- Never share personal information such as their full name, address, phone number, or passwords.
- Tell a member of staff or their parent/carer immediately if they see or receive anything online that upsets them.

- Never meet anyone in person whom they've only met online.
- Only use StudyBox devices and accounts with staff supervision and permission.
- Not install or download unauthorised apps, software, or games on StudyBox equipment.
- Follow staff instructions on online safety and digital etiquette.

c. Parents and Carers

Parents and carers are encouraged to:
- Support StudyBox's digital safety approach and reinforce safe online behaviour at home.
- Talk to their children about responsible internet use.
- Report any safeguarding or online safety concerns to StudyBox promptly.

4. Online Safety and Monitoring

- StudyBox uses appropriate filtering and monitoring systems to protect children from harmful online content.
- All use of StudyBox's internet and devices may be monitored for safety, security, and compliance.
- Monitoring data will be used solely for safeguarding and system security purposes.
- Any breach of this policy may result in restricted access, disciplinary action, or referral to external agencies (e.g. police, LADO, local authority).

5. Data Protection and Privacy

- All users must handle data in line with the Data Protection Act 2018 and StudyBox's Data Protection Policy.
- Personal data, photos, and videos of pupils must only be used or shared with parental consent and for approved purposes.
- Devices used for teaching or administrative purposes must be password protected and locked when unattended.

6. Reporting Concerns

All users must immediately report:
- Any incident that could compromise online safety.
- Accidental or deliberate access to inappropriate material.
- Concerns that another person is at risk or being harmed online.

Reports should go directly to the Designated Safeguarding Officer (DSO):

Designated Safeguarding Officer (DSO):
Shannon Hill – 07436 073299 / 020 8642 8884 / shannon@studybox.london

7. Breaches and Sanctions

- Staff: Breaches may lead to disciplinary action, including dismissal or referral to the LADO.
- Pupils: Breaches may result in loss of device privileges, parental contact, or safeguarding intervention.
- Volunteers/Visitors: Breaches may result in withdrawal of access or removal from the premises.

8. Review and Approval

This policy will be reviewed annually or sooner if statutory guidance changes.