HIAC

📄 Acceptable Use Policy (Staff)

High Impact Academic Coaching Ltd
89–90 Paul Street, London, EC2A 4NE
Company Number: 12386860
📧 safeguarding@highimpactacademiccoaching.com
🌐 www.highimpactacademiccoaching.com
Audience: All Staff
Owner: Designated Safeguarding Lead (DSL)

---

1. Purpose

This policy outlines the expectations for staff use of HIAC's digital systems, devices, and internet services. It ensures that all technology is used safely, legally, and in a manner that supports safeguarding, the Prevent Duty, and professional conduct.

---

2. Scope

This policy applies to all HIAC staff, contractors, and volunteers who access our systems or work with children and young people (C/YP) using digital tools.

---

3. Safeguarding & Prevent Duty Alignment

Staff must use technology in ways that:

- Protect children from online harm, abuse, exploitation, and radicalisation
- Promote British values and respectful dialogue
- Prevent exposure to extremist content or ideologies
- Support the emotional and physical safety of learners

---

4. Acceptable Use Includes

- Accessing educational platforms and resources
- Communicating professionally with learners, colleagues, and parents
- Using devices and systems for planning, assessment, and safeguarding documentation
- Promoting digital literacy and safe online behaviours among learners

---

5. Unacceptable Use Includes

- Accessing, creating, or sharing content that is illegal, extremist, pornographic, or discriminatory
- Using personal devices or accounts to communicate with learners outside approved platforms
- Sharing confidential learner data without authorisation
- Installing unauthorised software or disabling security settings
- Using work systems for personal gain or political promotion
- Attempting to bypass filters, monitoring systems, or firewalls

---

6. Security & Data Protection

- Staff must use strong passwords and keep them confidential
- Devices must be locked when unattended
- Personal data must be stored and shared in line with HIAC's Data Protection Policy and UK GDPR
- All safeguarding records must be stored securely and accessed only by authorised personnel

---

7. Monitoring & Compliance

- HIAC reserves the right to monitor digital activity for safeguarding and operational purposes
- Breaches of this policy may result in disciplinary action, referral to the DSL, or external investigation
- Serious breaches may be referred to the Local Authority Designated Officer (LADO), police, or Prevent team

---

8. Reporting Concerns

- Staff must report any safeguarding, cyberbullying, or Prevent-related concerns to the DSL immediately
- Suspicious emails, phishing attempts, or system vulnerabilities must be reported to IT support

---

9. Acknowledgement & Agreement

All staff must read, understand, and sign this policy before accessing HIAC systems. By signing, staff agree to uphold the principles of safeguarding, the Prevent Duty, and responsible digital conduct.

Year-on-Year Document Review

Review Date	Reviewer Name	Changes Made / Notes	Next Review Date
01/10/25	Kris Geddes	N/A	01/10/26