Busy Bees.
Education and Training

Internet and E-Safety Policy

15 June 2026

Mission, Vision and Values

Mission

Progressing lives through pioneering education.

Vision

Empowering people to unlock their full potential and achieve lasting success.

Values

Care

Expertise

Innovation

Accountability

Busy Bees Education and Training

Contents

1. Policy Statement

Busy Bees Education and Training (BBET) is committed to creating a safe, inclusive and secure digital environment where learners, staff and stakeholders can learn, work and communicate safely.

BBET recognises that technology and online platforms play a significant role in education, training and workplace learning. While digital technologies provide valuable opportunities for learning, collaboration and communication, they may also expose individuals to safeguarding, welfare, cyber security and reputational risks.

Online safety forms an integral part of BBET's safeguarding arrangements and is embedded throughout the learner journey, staff practice and organisational culture.

BBET is committed to:

- protecting learners and staff from online harm;
- promoting safe, responsible and respectful online behaviour;
- developing digital resilience and cyber awareness;
- supporting safe use of emerging technologies;
- responding promptly and effectively to online safety concerns;
- maintaining secure and resilient digital systems;
- ensuring compliance with relevant legislation and regulatory requirements.

Online safety is everyone's responsibility.

2. Scope

This policy applies to all stakeholders working with or on behalf of BBET including:

- All BBET employees and Governors including temporary, part-time and full-time staff, paid and unpaid volunteers.
- All prospective and current learners and alumni
- Employers hosting learners, partner organisations, contractors and external visitors

Online safety responsibilities apply across:

- Online, remote or blended learning provision
- Employer workplaces, BBET premises and external training venues
- Early years placements and childcare settings
- BBET systems, platforms, devices and communication channels including:
  - Microsoft Teams
  - Virtual Classrooms
  - E-portfolio systems
  - Assessment platforms
  - Email and digital communications
  - Social media, and
  - Mobile devices and personal technology used for BBET activities.

3. Policy Principles

BBET's approach to online safety, internet safety and e-safety is underpinned by the following principles:

- To promote a culture of safe, respectful, inclusive and responsible online behaviour across all learning, working and digital environments.
- To support learners and staff to use technology confidently, safely and effectively, whilst understanding and managing online risks.
- To protect learners and staff from online harm, abuse and exploitation, including cyberbullying, grooming, harassment, impersonation, fraud, online coercion, sexual exploitation, radicalisation, extremist influence, misinformation and exposure to harmful or inappropriate content.
- To recognise online safety as a key component of safeguarding and learner welfare, ensuring online risks are identified, reported and managed effectively.
- To develop digital literacy and cyber awareness, enabling learners and staff to evaluate online information, recognise potential risks and make informed decisions when using digital technologies.
- To provide clear, accessible and effective procedures for reporting, recording and responding to online safety concerns, incidents or breaches.
- To ensure staff understand their responsibilities for maintaining professional online conduct, appropriate digital communication and safe use of technology.
- To comply with relevant legislation and statutory guidance, including UK GDPR, the Data Protection Act 2018, the Online Safety Act 2023, Keeping Children Safe in Education, the Prevent Duty and safeguarding legislation.
- To promote digital resilience, challenging extremist narratives, and ensure concerns relating to online radicalisation or harmful influences are identified, reported and escalated appropriately.
- To promote responsible digital citizenship, encouraging learners and staff to demonstrate respect and ethical behaviour when interacting online.
- To maintain secure, reliable and resilient digital systems through effective cyber security controls, access management, monitoring arrangements and alignment with recognised standards.
- To continuously monitor emerging technologies, online behaviours and digital risks, including artificial intelligence (AI), social media platforms, virtual environments and evolving cyber threats, adapting controls and support arrangements where necessary.

4. Definitions

Online Safety / E-Safety: safe and responsible use of technology and internet-enabled devices.

Cyberbullying: bullying or harassment via digital platforms.

Grooming: manipulation or exploitation through online or digital communication.

Sexting / Sharing Nude or Semi-Nude Images: sending, receiving or sharing sexual content.

Phishing / Cybercrime: attempts to steal data or compromise systems.

Digital Footprint: information created through online activity.

5. Online Safety and E-Safety Risks

BBET recognises that learners and staff may be exposed to a wide range of online safety risks across educational, workplace, social and personal digital environments, including exposure to:

- online radicalisation, extremism and harmful ideological influence;
- violent, hateful, discriminatory or inappropriate content;
- pornography, sexual abuse, sexual exploitation and the sharing of nude or semi-nude images;
- misinformation, disinformation and manipulated content, including AI-generated content and deepfakes;
- online gambling, gaming-related harms and financial exploitation;
- self-harm or suicidal related content.
- online grooming, exploitation, coercion or inappropriate contact;
- criminal exploitation, including county lines activities through digital platforms;
- cyberbullying, online abuse, harassment, trolling and online intimidation;
- phishing, fraud, scams, and cybercrime;
- Malware, hacking, data breaches and identity theft.
- privacy breaches, data theft and unauthorised sharing of personal information;
- excessive or unhealthy use of technology that may negatively affect wellbeing, mental health or learning.

BBET recognises that online risks are continually evolving and will review emerging threats and technologies as part of its safeguarding and risk management arrangements.

6. Internet Safety and Appropriate Use

BBET recognises that access to the internet and digital platforms is an essential part of modern learning and employment. However, online activity can also expose individuals to safeguarding, welfare, cyber security and reputational risks.

Learners and staff are expected to use the internet, digital technologies and online platforms safely, responsibly, ethically and in accordance with applicable laws, organisational policies and professional standards.

Users must:

- use BBET systems, devices and learning platforms for legitimate educational and business purposes;
- treat others with respect and professionalism when communicating online;
- protect confidential information from unauthorised access or disclosure;
- access only appropriate, lawful and work-related content whilst using BBET systems and platforms;
- comply with BBET policies relating to safeguarding, data protection, acceptable use, social media and information security;
- report any online safety concern, cyber security incident or inappropriate online activity promptly.

Users must not:

- access, create, store or promote illegal content;
- distribute harmful material;

- engage in cyberbullying;
- share offensive or discriminatory content;
- bypass security controls;
- misuse BBET systems.

The deliberate accessing, creating, storing, sharing or promoting of illegal, offensive, discriminatory, extremist, abusive, sexually explicit or harmful content through BBET systems or in connection with BBET activities may result in malpractice or disciplinary action and, where appropriate, referral to external agencies.

7. Online Safety in Learning Delivery

BBET embeds online safety throughout the learner journey and promotes safe digital practices across all learning environments, including face-to-face, remote, blended and workplace learning.

Online safety is embedded throughout:

- virtual classrooms and video conferencing platforms;
- Microsoft Teams meetings and online tutorials;
- progress reviews and teaching sessions;
- e-portfolio and assessment system activities;
- email, messaging and communication platforms;
- employer engagement including digital environments and workplace systems;
- enrichment activities personalised to learners;
- online research, independent study and digital learning resources.

Staff are expected to:

- maintain professional boundaries and appropriate online conduct;
- use approved BBET systems and communication channels;
- reinforce online safety messages during delivery and progress reviews;
- challenge unsafe or inappropriate online behaviour where identified;
- remain vigilant to indicators of online harm, exploitation or cyber risk;
- report concerns in accordance with BBET safeguarding procedures.

Learners will receive online safety guidance during induction and throughout their programme to support safe and responsible participation in digital learning.

BBET will promote online safety during remote learning, Teams meetings, e-portfolio use, online assessment, email communication and employer digital environments. Staff are expected to maintain professional boundaries and appropriate conduct.

This approach ensures that learners are equipped to identify online risks, make informed decisions, protect themselves and others, and access support when concerns arise.

8. Social Media and Digital Communication

Staff and learners are expected to use social media and digital communication platforms responsibly and in a way that upholds BBET's values and professional standards.

Staff must maintain clear professional boundaries at all times and must not:

- establish inappropriate personal relationships with learners via social media;
- communicate with learners through personal social media accounts;
- share confidential or sensitive information online;
- engage in inappropriate conversations or behaviour that could compromise safeguarding, confidentiality or professional integrity.

Communication with learners should be through approved BBET systems and be professional, appropriate and relevant to learning and support activities.

BBET recognises that inappropriate online conduct, whether inside or outside working hours, may impact learner safety, organisational reputation and professional standards and may therefore be subject to investigation.

9. Cyber Security and Data Protection

BBET is committed to maintaining secure and resilient digital systems that protect learners, staff, organisational information and learning records from unauthorised access, loss, misuse or cyber-attack.

All users are responsible for contributing to cyber security by:

- using strong passwords and multi-factor authentication where available;
- protecting devices from unauthorised access;
- securely storing and transmitting personal or sensitive information;
- remaining vigilant to phishing emails, suspicious links and cyber threats;
- reporting suspected cyber incidents immediately;
- complying with BBET data protection, information security and acceptable use requirements.

BBET maintains appropriate technical and organisational controls, including access management, security monitoring, data protection measures and cyber security arrangements aligned to recognised good practice standards.

10. Artificial Intelligence, Misinformation and Emerging Risks

BBET recognises that emerging technologies, including artificial intelligence (AI), generative AI tools, deepfakes, virtual environments and social media algorithms, present both opportunities and risks.

Learners and staff will be supported to:

- critically evaluate information obtained online;
- identify misinformation, disinformation and manipulated content;
- understand the ethical and responsible use of AI technologies;
- recognise potential safeguarding and cyber risks associated with emerging technologies;
- use AI tools in accordance with BBET's AI and Plagiarism Policy.

11. Prevent and Harmful Online Content

BBET recognises that online environments and social media may expose learners and staff to extremist narratives, radicalising influences, harmful ideologies, conspiracy theories and other content that may present safeguarding risks.

BBET supports learners by:

- promoting British Values, critical thinking and respectful debate;
- developing digital resilience
- supporting learners to identify and challenge misinformation and extremist narratives;
- providing education relating to online safety, British Values and Prevent;
- maintaining appropriate filtering, monitoring and reporting arrangements; and
- ensuring concerns relating to online radicalisation are managed through safeguarding procedures.

Any concerns that an individual may be vulnerable to radicalisation, extremism or harmful online influence must be reported immediately to the Designated Safeguarding Lead (DSL) in line with the BBET Safeguarding & Child Protection Procedures and Prevent Policy.

12. Reporting Online Safety Concerns

BBET encourages all learners, staff and stakeholders to report online safety concerns immediately so that appropriate support and intervention can be provided.

All online safety concerns should be reported in accordance with BBET Safeguarding and Child Protection Procedures and, where appropriate, information security incident reporting processes. Concerns involving immediate risk of harm should be escalated urgently to the DSL and, where necessary, emergency services or external safeguarding agencies.

Staff should follow the 4 R's:

- **Recognise:** Identify signs of concern.
- **Respond:** Listen, reassure and remain calm.
- **Record:** Accurately document facts.
- **Report:** Report immediately to the DSL or DSO.

Staff must never:

- investigate concerns themselves;
- promise confidentiality;
- delay reporting.

13. Information Sharing

Information relating to online safety concerns may be shared where necessary to protect individuals from harm. Information sharing will comply with BBET's safeguarding principles, UK GDPR and Data Protection legislation.

14. Record Keeping

BBET will securely store and maintain accurate records of:

- online safety concerns;
- cyber incidents;
- safeguarding referrals;
- actions taken;
- outcomes achieved.

15. Roles & Responsibilities

Board / Governance

The Board is responsible for:

- ensuring effective oversight of online safety arrangements;
- receiving assurance regarding safeguarding and online safety;
- reviewing online safety risks and incidents;
- monitoring compliance with statutory requirements;
- ensuring sufficient resources are available.

Senior Leadership Team

The Senior Leadership Team is responsible for:

- promoting a strong culture of online safety;

- ensuring implementation of this policy;
- monitoring online safety performance;
- reviewing emerging risks;
- ensuring appropriate training is provided;
- supporting continuous improvement.

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- leading online safeguarding arrangements;
- receiving and reviewing online safety concerns;
- supporting staff with online safeguarding matters;
- making referrals where appropriate;
- monitoring trends and themes;
- reporting significant concerns to senior leaders.

Designated Safeguarding Officers (DSOs)

- DSOs support the DSL by:
- receiving safeguarding concerns;
- supporting investigations;
- maintaining records;
- monitoring learner welfare;
- acting in the absence of the DSL.

Regional Operations Managers

Regional Operations Managers are responsible for:

- ensuring coaches understand online safety responsibilities;
- monitoring compliance through quality assurance activity;
- reviewing trends and concerns;
- ensuring staff training is completed;
- escalating significant concerns.

Coaches and IQAs

Coaches and IQAs are responsible for:

- reinforcing online safety throughout delivery;
- monitoring learner wellbeing;
- identifying concerns;
- maintaining professional boundaries;
- reporting concerns promptly;
- supporting learners to stay safe online.

Learners

Learners are expected to:

- use technology responsibly;
- protect personal information;

- report concerns;
- treat others respectfully online;
- comply with BBET expectations;
- avoid sharing harmful or inappropriate content.

Employers

Employers are expected to:

- provide safe digital working environments;
- support apprentices to raise concerns;
- cooperate with safeguarding investigations;
- report concerns affecting apprentices.

16. Monitoring and Governance

Online safety arrangements are monitored through:

- safeguarding reports;
- incident reviews;
- quality assurance activity;
- learner and employer feedback;
- staff training compliance;
- governance oversight.

Themes and trends inform continuous improvement

17. Related Policies

This policy should be read alongside BBET's other policies and procedures including:

- Anti-Harassment and Anti-Bullying Policy
- Artificial Intelligence (AI) and Plagiarism Policy
- Critical and Serious Incident Policy and Process
- Data Protection Policy
- Equality, Diversity and Inclusion Policy
- Feedback, Compliments and Complaints Policy
- Health and Safety Policy
- Learner Code of Conduct
- Learner Inclusion Policy and Strategy
- Prevent Policy, Risk Assessment and Action Plan
- Safeguarding and Child Protection Policy
- Safeguarding and Child Protection Procedures
- Speak Up Policy
- Staff Code of Conduct

Contact

If you have any questions or suggestions regarding this policy, please contact:

Designated Safeguarding Lead

Busy Bees Education and Training

St Matthews, Shaftsbury Drive, Burntwood, WS7 9QP, UK.

Email: BBT.safeguarding@busybees.com

Statutory information

Busy Bees Education and Training Limited

Registered in England and Wales under Company Registration No. 03026494

Registered Office: St Matthews, Shaftsbury Drive, Burntwood, WS7 9QP, UK.

Email: enquiries@busybees.com

Review

This policy is:

- Monitored by senior leadership
- Reviewed at least annually, or in response to legislative changes or following updates to risk assessments or incidents
- Agreed and signed off by the CEO

Training and Roll Out

This policy is made available via the BBET website (busybeestraining.co.uk/policies) and SharePoint. Training will be made available via our Virtual Learning Academy (VLA) and/or during Face-to-Face or Teams meetings as part of ongoing staff development, along with our commitment to this policy.

Policy Owner: Designated Safeguarding Lead

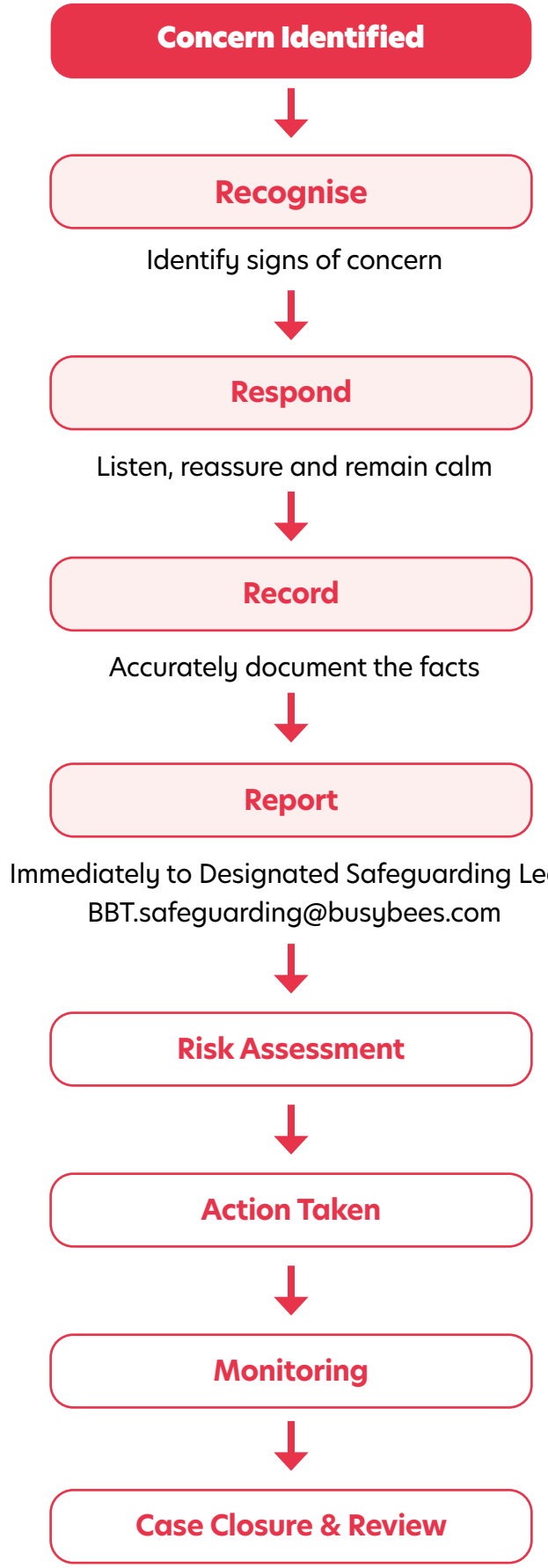
Ref: C10-Internet and eSafety Policy

Version: 1.0

Approval Date: 15th June 2026

Review Date: 30th June 2027

Appendix A: Online Safety Reporting Flowchart



Appendix B: Internet and eSafety Risk Indicators

The following indicators may suggest that a learner or staff member is experiencing online harm, digital exploitation, cyber-related abuse or unsafe internet use.

The presence of one indicator does not necessarily mean harm is occurring; however, patterns or multiple indicators should prompt concern and may require safeguarding intervention.

Behavioural Indicators

Potential warning signs may include:

- Sudden withdrawal, anxiety or distress following online activity
- Increased secrecy regarding device or internet use
- Reluctance to discuss online interactions
- Obsessive or excessive screen time
- Sudden disengagement from learning or communication
- Significant changes in mood, behaviour or confidence
- Fear of checking messages, notifications or emails
- Social isolation or avoidance of peers
- Increased aggression, irritability or emotional dysregulation

Indicators of Cyberbullying or Harassment

Signs may include:

- Distress after viewing messages or social media
- Avoidance of digital platforms previously used confidently
- Evidence of threatening, humiliating or abusive messages
- Sudden loss of confidence or self-esteem
- Fear of specific peers, groups or online communities
- Emotional upset linked to group chats, gaming platforms or social media

Indicators of Grooming or Exploitation

Potential indicators include:

- Receiving gifts, money or rewards from unknown individuals
- Secretive communication with older or unknown persons
- Use of multiple hidden or anonymous accounts
- Pressure to share personal details, images or videos
- Sexualised language or behaviour inappropriate to age/maturity
- Attempts to isolate learner from support networks
- Emotional dependence on online relationships

Indicators of Online Radicalisation or Harmful Influence

Signs may include:

- Sudden fixation on extremist ideologies or conspiracy content
- Repetitive sharing of extremist, hateful or violent content
- Increasingly rigid or intolerant views
- Withdrawal from family, peers or normal support systems
- Use of extremist language or symbols
- Participation in harmful online communities or forums

Indicators of Cybercrime, Fraud or Digital Exploitation

Warning signs may include:

- Suspicious financial activity or unexplained purchases
- Device compromise, hacking or loss of access
- Requests to share passwords or authentication codes
- Clicking suspicious links or downloading unknown files
- Reports of phishing, scams or identity theft
- Unusual account activity or impersonation

AI, Deepfake and Misinformation Risks

Indicators may include:

- Sharing manipulated or false content as fact
- Inability to identify reliable sources
- Exposure to AI-generated scams or impersonation
- Use of AI to deceive, harass or mislead others
- Belief in false narratives driven by algorithmic content

Where concerns arise, staff must follow BBET safeguarding or incident reporting procedures immediately.

Appendix C: Learner Online Safety Expectations

BBET expects all learners to use the internet, digital devices and online platforms safely, responsibly and respectfully.

Learners are expected to:

Use Technology Responsibly

Learners should:

- Use BBET systems, e-portfolio platforms and learning technologies appropriately
- Use the internet safely, legally and responsibly
- Protect passwords, accounts and personal information
- Think critically about information found online
- Use technology to support learning positively

Treat Others Respectfully Online

Learners must:

- Communicate respectfully in all digital spaces
- Show kindness and professionalism in messages, chats and online meetings
- Respect the rights, privacy and dignity of others
- Report cyberbullying, harassment or harmful behaviour

Learners must not:

- Bully, threaten or harass others online
- Share abusive, discriminatory or offensive content
- Impersonate others
- Share private content without permission

Stay Safe Online

Learners should:

- Be cautious when communicating with unknown individuals online
- Avoid sharing personal or sensitive information
- Be alert to scams, phishing and fraud
- Report suspicious activity immediately
- Block and report harmful or inappropriate contact

Use AI and Digital Tools Responsibly

Learners are expected to:

- Use AI tools ethically and in line with BBET policies
- Be transparent when AI tools are used in assessments
- Avoid using AI for plagiarism, cheating or misrepresentation
- Check the accuracy of AI-generated information

Report Concerns

Learners must report immediately if they experience or witness:

- Cyberbullying
- Online harassment
- Grooming or exploitation
- Exposure to harmful or extremist content
- Fraud, scams or cybercrime
- Inappropriate online contact
- AI misuse, impersonation or deepfake abuse

Concerns can be reported to:

- BBT.safeguarding@busybees.com
- Designated Safeguarding Lead (DSL)
- Designated Safeguarding Officer (DSO)
- Development Coach
- Regional Operations Manager

BBET encourages learners to speak up early. Reporting concerns helps protect both individuals and the wider learning community.

Appendix D: Staff Digital Conduct Standards

All BBET staff are expected to model safe, professional and responsible digital behaviour at all times. These standards apply to all online interactions involving learners, colleagues, employers and external stakeholders.

Professional Communication

Staff must:

- Use approved BBET systems, platforms and communication channels wherever possible
- Maintain professional, respectful and appropriate digital communication
- Ensure communication is relevant to learning, welfare or business purposes
- Communicate in a manner that protects professional boundaries

Staff must not:

- Use personal social media or private messaging platforms to communicate with learners
- Share personal contact details unnecessarily
- Engage in inappropriate, overly familiar or unprofessional communication
- Communicate with learners outside reasonable working boundaries unless safeguarding concerns require immediate action

Professional Boundaries

Staff must:

- Maintain clear professional boundaries in all digital environments
- Avoid dual relationships or inappropriate online familiarity
- Avoid engaging with learner personal content where unnecessary

Staff must not:

- Add or accept learners on personal social media accounts
- Send or request personal images or videos
- Participate in inappropriate chats, jokes or content sharing
- Engage in behaviour that could be perceived as grooming, favouritism or exploitation

Data Protection and Security

Staff must:

- Protect learner data and confidential information
- Use strong passwords and secure authentication methods
- Lock devices when unattended
- Report data breaches or cyber concerns immediately
- Follow BBET data protection, GDPR and IT policies

Staff must not:

- Share passwords
- Store confidential data insecurely
- Access information without legitimate reason
- Forward sensitive learner data to personal devices or accounts

Online Learning Delivery Standards

When delivering online learning, staff must:

- Use approved platforms such as Teams or authorised learning systems
- Maintain professional conduct equivalent to face-to-face delivery
- Ensure online sessions are safe, respectful and appropriately supervised
- Challenge inappropriate online behaviour promptly
- Monitor chat functions and digital interactions where possible

Artificial Intelligence and Emerging Technology

Staff must:

- Use AI responsibly and ethically
- Verify AI-generated outputs before using them professionally
- Ensure AI tools do not compromise learner confidentiality
- Support learners to use AI appropriately

Staff must not:

- Input confidential learner information into unauthorised AI tools
- Use AI to generate misleading feedback or records
- Rely solely on AI without professional judgement

Breaches of digital conduct standards may result in disciplinary action.

Appendix E: Legislation and Statutory Guidance

This policy has been developed with reference to statutory safeguarding, Prevent, data protection and online safety legislation and guidance including:

- Adult Support and Protection (Scotland) Act, 2007
- Apprenticeships, Skills, Children and Learning Act, 2009
- Care Act, 2014
- Childcare Act, 2006
- Children Act, 1989 and 2004
- Children and Families Act, 2014
- Children, Young People and Families Plan (2024-2027)
- Children and Young People (Jersey) Law, 2022
- Children and Young People (Scotland) Act, 2014
- Children (Guernsey and Alderney) Law, 2008
- Children (Jersey) Law, 2002
- Counter-Terrorism and Security Act, 2015 (Prevent Duty)
- Criminal Justice (Children and Juvenile Court Reform) (Bailiwick of Guernsey) Law, 2008
- Data Protection Act, 2018
- General Data Protection Regulations (GDPR) UK
- Department for Education Apprenticeship Funding Rules
- Domestic Abuse Act, 2021
- Early Years Foundation Stage Statutory Framework, 2025
- Education Act, 2005
- Education and Skills Act, 2008
- Education (Scotland) Act, 1980
- Equality Act, 2010
- Female Genital Mutilation Act, 2023
- Further and Higher Education Act, 1992
- Getting it right for every child (GIRFEC)
- Health and Care Act, 2022
- Health and Safety at Work etc. Act, 1974
- Health and Social Care Act, 2012
- Human Rights Act, 1998
- Information sharing: Advice for Practitioners Providing Safeguarding Services, 2024
- Keeping Children Safe in Education, 2025
- Mandatory reporting of Female Genital Mutilation, 2015
- Mental Capacity Act, 2005
- National Guidance for Child Protection in Scotland, 2023
- Ofsted Education Inspection Framework
- Ofsted Review of Sexual Abuse in Schools and Colleges, 2021
- Online Safety Act, 2023
- Protection of Freedoms Act, 2012
- Protection of Vulnerable Groups (Scotland) Act, 2007
- Safeguarding Vulnerable Groups Act, 2006
- SEND Code of Practice, 2015
- Sexual Offences Act, 2003
- What to do if you're worried a child is being abused: advice for practitioners, 2015
- Work-based learners and the Prevent statutory duty, 2021
- Working Together to Safeguard Children, 2026