



TechNative Safeguarding Policy

Section 1: Policy Statement and Scope

1.1 Purpose and Commitment

TechNative Digital is committed to providing a safe, inclusive, and supportive environment for all learners, staff, and stakeholders across every programme we deliver. Safeguarding is embedded in our organisational culture, learner experience, and quality assurance systems. We aim to identify and respond to harm proactively, ensuring all staff and learners understand their rights and responsibilities. This includes protecting individuals from abuse, neglect, exploitation, discrimination, and other forms of harm — both offline and online. We also recognise the importance of promoting mental wellbeing and psychological safety as part of a broader safeguarding culture.

This policy is designed to:

- Meet statutory safeguarding requirements across education, funding, and inspection frameworks;
- Reflect current best practice and evolving risks in adult and youth education;
- Apply across all government-funded, commercial, and employer-led programmes;
- Be consistent with and supported by the following frameworks:
 - **Learning Support Strategy** – ensuring that learners with additional or complex needs are identified early and supported throughout;
 - **Careers Strategy** – ensuring learners are safeguarded during work placement and progression activities;
 - **Quality Strategy** – ensuring safeguarding is continuously monitored and forms part of our QIP and inspection readiness;
 - **Health and Safety Policy** – providing safe systems of work in physical and digital spaces;
 - **Data Privacy Policy and Privacy Notice** – governing the lawful processing, sharing, and protection of learner data;
 - **Carbon Reduction Plan** – reflecting our commitment to low-risk, sustainable, and ethical delivery models (e.g. remote-first provision).

1.2 Scope

This policy applies to:

- All TechNative staff, tutors, mentors, freelance contractors, board members, and delivery partners;
- All learners and programme participants, regardless of age, background, or funding stream;
- All delivery models (in-person, online, hybrid) and all programme types (government-funded, commercial, employer-sponsored, etc.);
- All current and future locations of delivery, including but not limited to West Sussex, East Sussex, Brighton & Hove, and Greater London.



1.3 Legal and Regulatory Framework

This policy is informed by the following statutory and inspection guidance:

- Children Act 1989 & 2004
- Care Act 2014
- Equality Act 2010
- Safeguarding Vulnerable Groups Act 2006
- Education Act 2002
- Prevent Duty (Counter-Terrorism and Security Act 2015)
- Working Together to Safeguard Children (2023)
- Keeping Children Safe in Education (2023)
- Ofsted Education Inspection Framework (EIF)
- Cyber Essentials and GDPR principles
- Pan-Sussex Multi-Agency Safeguarding Procedures (where applicable)

This policy is reviewed annually and updated in response to:

- Changes in legislation or funding guidance;
- Feedback from learners or staff;
- Recommendations from the Quality Improvement Plan (QIP);
- Developments in local, regional, or national safeguarding practice.

Section 2: Roles and Responsibilities

Section 2.1: Designated Personnel

To maintain a safe, compliant, and responsive safeguarding environment, TechNative has appointed the following key roles. Each role is embedded in our wider safeguarding system and accountable under Ofsted, DfE, and local authority frameworks.

Designated Safeguarding Lead (DSL)

The DSL has overall accountability for safeguarding across the organisation. They:

- Hold (or are working towards) a Level 3 Safeguarding qualification
- Lead on all safeguarding case management, policy implementation, referrals, and compliance
- Chair safeguarding case reviews and maintain the safeguarding log and dashboard
- Liaise with:
 - Local authority safeguarding partnerships (e.g. MASH)
 - Commissioners and contract managers
 - Ofsted inspectors during monitoring or inspection visits
- Monitor Prevent risks and lead the organisation's Prevent strategy
- Coordinate with the Health and Safety Lead and Data Protection Officer to ensure alignment



Deputy DSL(s)

Appointed deputies ensure safeguarding coverage and operational continuity. They:

- Are trained to the same level as the DSL
- Support incident triage, staff training, and referral management
- Take over DSL responsibilities in their absence
- Contribute to safeguarding audits, learner feedback analysis, and updates to the QIP

Senior Leadership Team (SLT)

The SLT provides strategic oversight and ensures that safeguarding is:

- Embedded in all decision-making, planning, and programme design
- Monitored through QA structures, CPD, and board reporting
- Adequately resourced and governed across all delivery formats and partnerships
- Reviewed in the Self-Assessment Report (SAR) and Risk Register

Tutors and Mentors

Tutors and mentors are the frontline identifiers of safeguarding risks. They are required to:

- Complete safeguarding, Prevent, and online safety training before delivery
- Model safe and inclusive professional behaviours
- Respond appropriately to disclosures and report all concerns without delay
- Collaborate with the DSL and LSC to implement safeguarding actions, learning plans, and learner check-ins
- Use approved communication channels and maintain digital conduct standards

Learner Success Managers

The LSMs supports safeguarding by:

- Identifying at-risk learners during onboarding
- Co-developing Individual Learning Plans (ILPs) that incorporate safeguarding needs
- Conducting wellbeing check-ins and contributing to case reviews
- Ensuring learners from priority groups (e.g. unemployed, SEND, NEET) receive tailored pastoral care
- Working closely with the Inclusion Lead, Tutors, and DSL

Designated SEND and Inclusion Lead

This role advises on safeguarding risks specific to:

- Neurodivergent and disabled learners
- Learners requiring adjustments, accessible materials, or trauma-informed approaches
- Intersectional vulnerabilities (e.g. dual diagnosis, language barriers, digital exclusion)



They contribute to ILPs and staff CPD, and co-review complex cases with the DSL.

Cybersecurity and Data Compliance Lead

This role oversees:

- Implementation of Cyber Essentials security controls
- Secure configuration of online delivery platforms (Zoom, Slack, Notion, etc.)
- Monitoring of digital risks and reporting on system integrity
- Collaboration with the DSL on digital safeguarding risks (e.g. grooming, impersonation, data leaks)

Section 2.2: Training and Development

Safeguarding competence is an organisational priority at TechNative. All staff — including contractors and partners — must demonstrate safeguarding awareness and confidence appropriate to their role. We deliver this through structured onboarding, mandatory CPD, and live monitoring of training compliance.

Mandatory Training for All Staff

All TechNative staff, freelancers, and delivery partners must complete safeguarding training **before any learner-facing activity**. This includes:

- **Level 1 Safeguarding Awareness**
- **Prevent Duty Awareness**
- **Cybersecurity and Online Safety Essentials**
- **Whistleblowing and Escalation Procedures**
- **Low level concerns procedures enables staff to share any concern - no matter how small**
- **Code of Conduct for Working with Learners**
- **Safer Recruitment (for staff involved in hiring or interviews)**

Completion is tracked centrally by the DSL and reviewed in quality audits and termly CPD updates.

Training courses to be completed include

[Introduction to Safeguarding Adults \(Level 1\)](#)

[Prevent Duty Training | Online Course For Education](#)

[Equality, Diversity & Inclusion \(EDI\) Training | Online Course](#)

[GDPR Training | Online City & Guilds Course](#)



Annual Refresher and Continuous CPD

Safeguarding is embedded in the annual CPD cycle. All staff must complete refresher training every 12 months, covering:

- Updates to statutory guidance (e.g. KCSIE, Prevent Duty, Working Together)
- Case reviews and lessons learned
- Local safeguarding risks or escalation routes (e.g. Sussex vs. London)
- Digital safeguarding risks (e.g. deepfakes, grooming, trolling)
- Equality, diversity, and inclusion (EDI) issues that overlap with safeguarding

Training is supplemented with case-based learning and micro-learning videos as needed.

DSL and Deputy DSL Requirements

The DSL and Deputy DSL(s) must:

- Hold or complete a **Level 3 Safeguarding for Designated Leads** qualification within 6 months of appointment
- Complete annual CPD on:
 - Advanced safeguarding case management
 - Channel and Prevent referral procedures
 - Emerging policy (e.g. AI harms, digital resilience)
- Lead training sessions and reflective debriefs with delivery staff

They also contribute to:

- DSL network or local multi-agency forums
- Sector-wide Prevent and safeguarding updates

Observation, Debrief, and Peer Learning

Safeguarding effectiveness is monitored through the QA system. This includes:

- **Lesson observations** focused on tutor safeguarding practice and inclusion
- **Tutor debriefs** to reflect on safeguarding concerns and support needs
- **Safeguarding CPD forums** for sharing trends and reviewing internal/external cases
- **Feedback loops** between the DSL, Quality Lead, and Learning Support Coordinator

These activities feed directly into the **QIP** (Quality Improvement Plan) and **SAR** (Self-Assessment Report), supporting TechNative's goal of continuous improvement and Ofsted readiness.

Section 3: Safeguarding Processes

3.1 Types of Abuse Recognised

TechNative recognises that safeguarding extends beyond child protection to encompass all learners, particularly those aged 18–25 or who are vulnerable due to SEND, socio-economic disadvantage, or other contextual risks.

We recognise the following types of abuse, as outlined in statutory guidance (KCSIE, Working Together 2023):

- Physical abuse
- Emotional abuse



- Sexual abuse or exploitation
- Neglect or self-neglect
- Domestic abuse and coercive control
- Financial abuse and fraud
- Online harms, including grooming, trolling, doxing, and exploitation
- Discriminatory abuse, including hate crime or cultural marginalisation
- Radicalisation and extremism (Prevent Duty)
- Sexual harassment or peer-on-peer abuse, both online and offline

Staff are trained to recognise signs of abuse across in-person and digital environments, in line with the Ofsted Education Inspection Framework (EIF) and Cyber Essentials principles and Adult Safeguarding Principles. In line with the Care Act 2014, TechNative applies the six principles of adult safeguarding: empowerment, prevention, proportionality, protection, partnership, and accountability

Safeguarding concerns may arise from cumulative vulnerabilities such as mental health needs, care experience, digital isolation, or housing insecurity.

3.2 Reporting and Escalation

- All safeguarding concerns — including suspicions, disclosures, or third-party reports — must be reported immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL.
- Concerns should be recorded using the [Safeguarding Concern Form \(Annex A\)](#) and submitted within the same working day.
- Reports are logged securely in the **Safeguarding Register**, stored in line with GDPR, DfE funding conditions, and TechNative's Privacy Notice.
- The DSL will:
 - Triage and assess each case;
 - Refer to external agencies where appropriate (e.g. MASH, Prevent/Channel, Police);
 - Record rationale, action taken, and follow-up steps;
 - Liaise with commissioners and, where required, escalate serious incidents to contract leads.
- Allegations against staff - TechNative follows statutory procedures including possible suspension or redeployment while investigations are ongoing. Where appropriate, referrals will be made to the Disclosure and Barring Service (DBS) and/or the Teaching Regulation Agency (TRA).

A **Serious Incident Flowchart** is made available to all staff, outlining clear response times and escalation protocols for:

- Allegations involving staff or tutors
- Safeguarding concerns within employer placements or projects
- Immediate safety risks, radicalisation concerns, or online abuse

Confidentiality is maintained at all stages, but safeguarding concerns override data protection rules where the safety or wellbeing of a learner or other party may be at risk.



3.3 Monitoring, Audit, and Continuous Improvement

Safeguarding effectiveness is monitored through proactive QA and live case tracking:

- **Quarterly Safeguarding Audits**
Conducted by the DSL and reviewed by SLT. These assess case handling, training compliance, digital safety, and Prevent activity.
- **Learner Feedback and Voice**
Learner surveys (onboarding, midpoint, and exit), debriefs, and tutorial discussions include safeguarding indicators such as:
 - Feeling safe in learning spaces
 - Knowing how to raise a concern
 - Perception of tutor behaviour and support
- **Case Review Meetings**
Complex, repeated, or unresolved concerns are reviewed by the DSL with relevant staff (e.g. LSC, Inclusion Lead, Tutors). Actions are logged and reflected in CPD, ILPs, or delivery plans.
- **Safeguarding Improvement Plan**
Trends, themes, and feedback feed directly into TechNative's **Quality Improvement Plan (QIP)** and **Self-Assessment Report (SAR)**. This ensures safeguarding remains live, learner-informed, and accountable at leadership and governance level.

Section 4: Safe Delivery – Online, Hybrid and In-Person

TechNative is committed to creating and maintaining safe learning environments across all delivery formats. Safeguarding principles must be applied equally across physical and virtual spaces, ensuring accessibility, inclusion, and protection for all learners. These expectations are consistent with our Health and Safety Policy, Data Privacy Notice, and Cyber Essentials commitments.

4.1 Digital Safeguarding and Cybersecurity

We recognise that remote and hybrid delivery bring unique safeguarding risks, including isolation, online grooming, trolling, and digital abuse. To mitigate these:

- **All platforms** (e.g. Zoom, Slack, Notion, Canvas, Google Workspace) must be:
 - Password-protected
 - GDPR-compliant
 - Configured to limit unauthorised access and ensure private chat/data security
 - Managed in line with Cyber Essentials standards
- **Online Learning Code of Conduct (Annex B)** is issued to all learners and staff, covering:
 - Appropriate language and behaviour
 - Expectations for camera/microphone use
 - Zero tolerance for bullying, harassment, or exclusion
 - Guidance on how to report digital misconduct
- **Moderation of Digital Spaces**
 - Online forums and chat threads are monitored weekly by tutors and/or the DSL team



- o Chat history is retained securely in line with the Safeguarding Register and GDPR
 - o Breakout rooms or unsupervised group calls are only used under strict moderation
- **Live Monitoring**
 - o All live sessions are delivered by trained tutors, with support from LSA/mentors where possible
 - o Tutors are trained to recognise digital risk indicators (withdrawal, disengagement, distress)
 - o Any signs of concern are flagged to the DSL immediately for follow-up

4.2 In-Person Delivery and Venue Safety

- **Pre-Delivery Venue Risk Assessments** must be completed and logged by the DSL or H&S Lead. These assessments include:
 - o Venue security and accessibility
 - o Lone working protocols and signage
 - o Emergency evacuation procedures and health & safety provisions
- **Safeguarding Oversight**
 - o At least one **trained first aider** must be present at any delivery venue
 - o DSL or Deputy DSL is on-call during in-person delivery periods
- **Attendance and Location Monitoring**
 - o All learners must sign in and out
 - o Unexplained absences trigger follow-up within one working day by the tutor and/or LSC
 - o Repeat absence is escalated to the DSL if safeguarding risk is suspected

4.3 Learner Safeguarding and Induction Modules

All learners complete a safeguarding induction before beginning any Skills Bootcamp. This includes:

- What safeguarding is and why it matters
- How to report concerns or disclosures
- Contact details for the DSL and Deputy DSL
- Prevent Duty awareness (e.g. how to spot extremist content or hate speech)
- Online Code of Conduct expectations
- Digital privacy, safe online learning, and managing screen time
- Safeguarding in the curriculum - and how tutors integrate digital safety respectful relationships

Reinforcement During Weeks 1–2:

- Recap discussion at first live session
- Group agreement building (e.g. classroom charter or Slack pledge)
- Opportunity for anonymous questions or check-ins

Section 5: Supporting Vulnerable Learners

TechNative is committed to proactively identifying and supporting learners at risk of disengagement, discrimination, mental ill health, or harm. This includes those with SEND, language barriers, neurodivergence, long-term health conditions, care experience, or socio-economic disadvantage.



Our safeguarding approach is embedded in our delivery model and guided by the **Learning Support Strategy**, ensuring early identification, timely support, and inclusive pathways to progression. We will actively promote at all times learner and staff wellbeing, Mental Health First Aiders, external services such as NHS 111 and Samaritans.

5.1 Identification and Early Support

Early identification is central to safeguarding and retention. We apply a structured risk-based approach from onboarding through to programme completion.

- **Safeguarding Risk Checks**

Conducted as part of learner onboarding and reviewed regularly by the DSL and Learning Support Coordinator (LSC). These cover:

- Health and wellbeing
- Device access, private space, learning environment
- Disclosure of SEND, neurodivergence, or trauma
- Employment, caring responsibilities, housing instability

- **Flagging and Alerts**

Where concerns arise, they are flagged via:

- Tutor onboarding notes
- ILP entries
- Attendance or engagement tracking
- Disclosures during check-ins or tutorials

High-risk learners are reviewed weekly at safeguarding briefings involving the DSL, LSC, and Inclusion Lead.

- **Individual Learning Plans (ILPs)**

Co-created with the learner, ILPs include:

- Goals and progression intentions
- Learning adaptations and accessibility needs
- Safeguarding considerations and referral history
- Contact preferences and risk alerts

ILPs are updated monthly and stored securely in line with the **Data Privacy Policy**.

5.2 Pastoral Support and Check-ins

We prioritise meaningful contact, consistent encouragement, and early intervention to maintain learner wellbeing.

- **All Learners**

- Receive structured fortnightly check-ins via Slack, live sessions, or email
- Are encouraged to use Slack threads or 1:1 check-ins to raise concerns

- **Priority and Vulnerable Learners** (e.g. unemployed, lone parents, young adults, learners with declared health or SEND needs)

- Are assigned a named contact (usually the LSC or a tutor with safeguarding knowledge)
- Receive weekly 1:1 or small group support
- Progress and engagement are reviewed fortnightly by the DSL and LSC
- Can access informal drop-in support with pastoral or wellbeing mentors

- **Missed Session Protocol**

- Any missed live session triggers a tutor follow-up within 1 working day



- If two or more sessions are missed without contact, the learner is flagged to the DSL and LSC for review and possible safeguarding intervention

5.3 Referrals and Signposting

When learners present safeguarding concerns, mental health needs, or complex risk factors, referrals are made with consent (unless risk overrides this).

- **Internal Referral Pathways**
 - Learning Support Coordinator
 - Inclusion Lead
 - Safeguarding Lead (DSL)
 - Employer Engagement Lead (where issues arise during workplace learning)
- **External Signposting** (voluntary)
 - Local IAPT or counselling services
 - Domestic abuse, housing or financial crisis services (e.g. CAB, DWP, local hubs)
 - LGBTQ+ and minoritised community support groups
 - Digital wellbeing and online safety resources
- **Consent and Confidentiality**
 - Where possible, learners give informed consent to referral or signposting
 - Exceptions apply in situations of serious risk or legal obligation (as defined in Section 9)
 - All referrals are logged securely, flagged for follow-up, and monitored via the Safeguarding Register

Section 6: Safer Recruitment and Conduct

TechNative is committed to building a safe and ethical working culture through rigorous recruitment, onboarding, and behavioural expectations. All staff, tutors, contractors, and partners undergo appropriate vetting and are held to the highest standards of professional conduct — especially when working with vulnerable or at-risk adults.

6.1 Recruitment Protocols

Recruitment is governed by our **Safer Recruitment Policy** and aligned with Ofsted expectations, funding contract requirements, and relevant safeguarding legislation.

- **Enhanced DBS Checks**
 - All staff, freelancers, or delivery partners engaged in regulated activity undergo an **Enhanced DBS check**, including the **adults' barred list**.
 - DBS renewals follow our contract cycle and validity review process.
 - Disclosure outcomes are reviewed by the DSL, and risk-assessed in line with our Safeguarding Policy.
- **Reference and Credential Verification**
 - Two references are required, including one from a recent employer or relevant client.
 - Right-to-work, professional qualifications, and employment history are verified during recruitment.
 - **Recruitment records** are retained securely, in line with our Data Privacy Policy and Annex D.



- **Barred List, Disqualification, and Suitability Risk Review**
 - No individual may be employed or deployed if:
 - Barred from regulated activity;
 - Under investigation for a relevant offence;
 - Identified as a safeguarding or reputational risk to learners;
 - In exceptional cases, written approval may be sought from the commissioning authority, and risk mitigation logged.
- **Safeguarding-Informed Interviews**
 - Every recruitment panel includes at least one **trained Safer Recruitment panel member**.
 - All interviews include:
 - Scenario-based safeguarding questions
 - Values-based assessments linked to our Code of Conduct
 - Questions tailored for remote or hybrid teaching responsibilities
- **Self disclosure**
 - All staff, contractors, and volunteers are required to confirm annually that they remain suitable to work with vulnerable adults and young people. Staff must disclose any arrests, charges, cautions, or changes in personal circumstances that may affect their suitability. The DSL reviews declarations and ensures risk assessments are undertaken where required.

6.2 Code of Conduct and Professional Standards

All staff must sign and adhere to the **TechNative Code of Conduct (Annex C)**, which outlines clear boundaries for behaviour, communication, and data handling. Key expectations include:

General Conduct

- Maintain professional, respectful, and inclusive relationships with learners.
- Protect learner confidentiality and avoid unprofessional disclosure.
- Avoid favouritism, excessive familiarity, or crossing role boundaries.

Working with Vulnerable Learners

- Adapt delivery for learners with SEND, trauma, or accessibility needs.
- Log all 1:1 pastoral conversations and escalate any concerns to the DSL or LSC.
- Reinforce safe learner behaviour, particularly where group dynamics or peer pressure may affect safety.

Digital Conduct (including remote tutors and contractors)

- All sessions must take place on **approved platforms**, using:
 - Waiting room and password controls
 - Screen share restrictions
 - Supervision or recording of 1:1 sessions (where applicable)
- Staff must not:
 - Use personal devices or social media to contact learners;
 - Save learner data outside of secure systems;
 - Hold unsupervised 1:1 calls unless approved and risk-assessed.

Whistleblowing and Escalation

- All staff must report breaches of the Code of Conduct immediately.
- **Annex E: Whistleblowing Procedure** is issued at onboarding and reviewed annually.



- Breaches are investigated by the DSL and may result in internal disciplinary action or external referral.

Section 7: Employer and Partner Responsibilities

TechNative recognises that safeguarding is a shared duty — particularly where learners engage with external employers, mentors, guest speakers, or placement providers. We maintain high safeguarding standards by setting clear expectations, conducting due diligence, and ensuring all parties understand their responsibilities in relation to learner safety.

These expectations apply equally across Skills Bootcamps, commercial offers, and co-designed projects.

Due diligence checks are conducted to confirm safeguarding compliance. All partners are required to adhere to TechNative's Safeguarding Policy. The DSL maintains oversight of safeguarding arrangements across all subcontracted provision.

7.1 Shared Safeguarding Responsibility

We ensure all employers and partners understand their responsibilities to safeguard learners through:

Safeguarding Onboarding for Employers

- All employer partners receive:
 - A summary of our **Safeguarding Policy**
 - Contact details for the **DSL and Deputy DSL**
 - A copy of the **Online Code of Conduct** (if digital contact is expected)
- Expectations are embedded into:
 - Memoranda of Understanding (MOUs)
 - Employer Agreements and Call-Off Contracts
 - Learning agreements or placement forms (if applicable)

Safeguarding Declaration (Annex G)

- Before any direct learner engagement (mentoring, interviews, placements), the employer must:
 - Appoint a named safeguarding contact
 - Confirm they have internal procedures for reporting harm, misconduct, or radicalisation
 - Acknowledge TechNative's escalation pathway and DSL contact protocol
 - Agree to notify us of any concerns, disclosures, or unsafe behaviour immediately

Prevent Duty Alignment

- Employers receive a **Prevent briefing pack** where relevant, and are expected to:



- o Flag any signs of extremist language, hate speech, or digital grooming
- o Support TechNative in addressing concerns that may arise during work-based interactions

Reporting & Escalation Protocol

- Any safeguarding concerns reported by or involving an employer must be escalated to the DSL immediately.
- A designated TechNative staff member coordinates the response, ensures records are logged, and notifies funders or local authorities where required.

7.2 Monitoring Placement Safety

All workplace learning environments — including placements, shadowing, and employer-hosted projects — are risk-assessed and actively monitored.

Risk Assessments (Annex H)

Before any learner begins placement:

- The **Placement Risk Assessment Form** is completed covering:
 - o Lone working
 - o Supervision and escalation routes
 - o Accessibility and inclusion
 - o Digital interaction and confidentiality controls
- The DSL or Operations Lead reviews and signs off the risk assessment before approval.

Ongoing Learner Contact

- Learners on placements receive:
 - o Weekly check-ins from their tutor or the LSC
 - o Access to escalation contacts if concerns arise
 - o Scheduled midpoint check-ins and end-of-placement reviews
- Tutors are responsible for:
 - o Noticing signs of distress, disengagement, or power imbalances
 - o Reporting missed sessions or concerning feedback to the DSL

Recording and Follow-Up

- All employer-related safeguarding notes, risk assessments, and learner issues are:
 - o Logged in the **Safeguarding Register**
 - o Monitored by the DSL and Employer Engagement Lead
 - o Reviewed mid- and post-programme to ensure lessons are captured

Section 8: Prevent and Online Safety

TechNative recognises that digital environments and social influence can expose learners to serious harm, including online grooming, hate speech, harassment, and radicalisation. We are committed to equipping staff and learners with the tools to understand, avoid, and report these risks, in line with the *Prevent Duty*, *Ofsted EIF*, and *Cyber Essentials*.



8.1 Prevent Duty Compliance

We fully comply with the **Counter-Terrorism and Security Act 2015**, which requires providers to prevent people from being drawn into terrorism.

Prevent Risk Assessment (Annex I)

- Reviewed annually by the DSL and included in the organisation's inspection readiness file
- Covers:
 - Delivery format risks (e.g. online radicalisation)
 - Local/regional threat levels
 - Learner demographics and digital behaviours
 - Placement and partner exposure

Staff Training

- All staff complete:
 - Prevent training on induction
 - Refresher training every 12 months
 - Scenario-based sessions on recognising extremist behaviours or content
- CPD logs are maintained by the DSL and reviewed as part of safeguarding audits

Learner Awareness

- Prevent is introduced as part of induction, then reinforced through curriculum content:
 - Digital citizenship and respectful online debate
 - Freedom of expression vs. hate speech
 - How to question harmful narratives
 - What to do if a peer or employer makes unsafe comments
- Prevent is discussed sensitively and framed through inclusion, empowerment, and civic responsibility

Escalation Protocol

- Any staff member with a concern about extremism or hate speech must report to the DSL immediately
- The DSL may escalate to the **Channel Panel**, local Prevent lead, or police
- All concerns are logged and reviewed as part of serious incident tracking

8.2 Online Safety and Digital Harm Prevention

Our commitment to digital safety applies to all learners, regardless of delivery format. This sits alongside our broader safeguarding and data protection responsibilities.

Acceptable Use and Behaviour

- All learners and staff must sign the **Online Learning Code of Conduct (Annex B)** covering:
 - Respectful communication and inclusive dialogue
 - Microphone/camera etiquette
 - Responsible use of breakout rooms, Slack, and collaborative tools
 - Prohibited behaviours (bullying, trolling, harassment, inappropriate messaging)



Platform Security and Configuration

- All platforms used must be:
 - Password-protected and access-restricted
 - Configured to limit screen sharing, chat abuse, and breakout misuse
 - Subject to regular audit as part of our Cyber Essentials compliance and safeguarding audit

Digital Safety Curriculum

Learners are supported to understand digital risk through:

- Live safeguarding sessions and induction content
- Slack Q&A and debriefs with tutors or LSC
- Topics covered include:
 - Sextortion and online grooming
 - Trolling, manipulation, and image-based abuse
 - Reporting peer harm or external exploitation
 - Managing digital footprints and consent online

Reporting and Support

- Learners are encouraged to report:
 - Harmful online content (even outside Bootcamp platforms)
 - Unsafe behaviour from peers or staff
 - Cyber incidents involving employers, mentors, or work-based settings
- Tutors and mentors escalate these to the DSL and log incidents securely

Record and Review

- All digital safeguarding cases are:
 - Logged in the Safeguarding Register
 - Reviewed in quarterly safeguarding audits
 - Tracked for themes that inform CPD, curriculum updates, and platform controls

Section 9: Data Protection and Record Keeping

TechNative maintains robust procedures to ensure all safeguarding information is collected, processed, stored, and shared in accordance with **UK GDPR**, **Cyber Essentials**, and local authority data handling requirements. These procedures also align with our **Privacy Policy**, **Data Privacy Notice**, and internal quality systems.

We recognise that safeguarding data often includes highly sensitive personal information and must be handled with heightened care, transparency, and accountability. All notes should be Notes are factual, timely, and written in line with professional standards for case recording.

9.1 Confidentiality and Secure Storage

Access Restrictions

- All safeguarding records are stored **digitally** in a secure, access-controlled environment
- Access is restricted to:
 - Designated Safeguarding Lead (DSL)
 - Deputy DSL(s)
 - Nominated Operations and Compliance Leads (where needed)



- Paper records are avoided unless explicitly required by contract, court, or investigation

Data Types Held

- Concern/disclosure forms (including Annex A submissions)
- Case notes, meeting logs, and follow-up actions
- Referrals and correspondence with local authorities or third-party services
- Risk assessments, escalation records, and closure summaries

Retention Period

- Safeguarding records are retained for **7 years after the learner's final engagement**
- Destruction follows a two-step process:
 - Logged in the Data Retention Log
 - Confirmed by the DSL and Data Protection Officer (DPO)

Platform and Security Compliance

All systems used to store safeguarding data must:

- Be GDPR compliant
- Use encrypted (SSL/TLS) data transmission
- Comply with **Cyber Essentials** security protocols
- Undergo regular access and permissions audits
- Restrict export or download of sensitive records without DSL/DPO authorisation

9.2 Information Sharing and Consent

Need-to-Know Principle

- Safeguarding information is shared strictly on a **need-to-know basis**, in accordance with GDPR Article 6 (Legal Obligation or Vital Interest)
- All staff are trained to understand:
 - When to escalate
 - What to log
 - What must be kept confidential

Learner Consent

- Wherever appropriate, learners are:
 - Informed of what will be shared, with whom, and why
 - Asked to confirm consent for referrals or follow-up conversations (especially for internal referrals like LSC or SEND support)
- Exceptions to consent apply when:
 - A learner is at serious risk of harm
 - There is a risk to another person
 - A legal or safeguarding obligation overrides privacy (e.g. risk of radicalisation)

Third Party Disclosures

- Information is only shared externally in accordance with:
 - Signed partnership agreements
 - MOU clauses
 - DfE and local authority contract requirements
- Examples include:
 - Notifying the local authority about a serious safeguarding incident
 - Sharing DSL reports with a commissioner upon request



- o Involving external services in referrals (e.g. MASH, Channel, Prevent)
- All disclosures are recorded in the **Safeguarding Register**, noting:
 - o Date and time
 - o Who the information was shared with
 - o Legal basis for sharing
 - o Summary of the shared content

Section 10: Monitoring and Continuous Improvement

TechNative views safeguarding as a continuous cycle of evaluation, adaptation, and accountability. We embed safeguarding across our quality systems to ensure our approach remains effective, compliant, and learner-led — supporting our ambitions for excellence and readiness for external scrutiny.

10.1 Annual Safeguarding Policy Review

An annual review of the full safeguarding framework is led by the **Designated Safeguarding Lead (DSL)**, in consultation with:

- Deputy DSLs
- Learning Support Coordinator (LSC)
- Operations and Compliance Lead
- Quality Lead
- Senior Leadership Team (SLT)
- Learner and employer representatives (where appropriate)

This review includes:

- Analysis of safeguarding trends and incident logs
- Audit outcomes and Prevent risk review
- Learner and tutor feedback (e.g. surveys, debriefs)
- Changes to guidance (e.g. KCSIE, Prevent Duty, Ofsted EIF)
- Regional and local safeguarding intelligence

The updated policy is:

- Signed off by the **Managing Director or Board**
- Shared with staff, learners, partners, and funders
- Accompanied by an implementation or CPD plan if substantive changes are made
- Version-controlled and appended to **Annex J (Review Log)**

10.2 Quality Assurance and Governance

Safeguarding is a core strand in TechNative's **Quality Assurance Framework**, ensuring it is embedded in curriculum, governance, and performance monitoring.

Our QA cycle includes:

Quarterly Safeguarding Dashboard (Annex K)

- DSL produces a dashboard capturing:
 - o Case volumes, trends, and response times
 - o Staff training and DBS compliance
 - o Learner voice findings and referral feedback
 - o Action status (e.g. open, escalated, resolved)



Observation and Training Logs

- All safeguarding-related CPD is tracked and reviewed termly
- Tutor observations explicitly review safeguarding awareness, escalation routes, and inclusive behaviour

Governance Oversight

- Safeguarding is a standing item in:
 - SLT strategy reviews
 - Termly Quality Review meetings
 - Board-level compliance briefings
- Risks or systemic issues are escalated to the **QIP (Quality Improvement Plan)** and summarised in the **SAR (Self-Assessment Report)**

10.3 Inspection and Contract Readiness

To meet Ofsted and contract expectations, TechNative maintains a **live inspection file** aligned to:

- Ofsted Education Inspection Framework (EIF)
- DfE Skills Bootcamp funding rules
- ESCC, WSCC, and GLA Skills funding contracts

This includes:

- Current Safeguarding Policy and annexes
- CPD/training tracker and staff responsibilities matrix
- DBS register and safer recruitment audit trail
- Live Prevent Risk Assessment
- Safeguarding referral and resolution logs
- Learner feedback reports and complaints tracker
- Evidence of policy implementation (e.g. staff declarations, employer briefings)

This file is reviewed every half-term by the DSL and Quality Lead, with updates reflected in the inspection dashboard and safeguarding improvement plan.

