

Safeguarding/ Prevent Policy

Policy Statement

Steadfast Training Ltd is strongly committed to practices that protect children, young people and adults at risk from abuse, neglect, significant harm or radicalisation.

Steadfast the Company recognise and accept their responsibility to develop the awareness of the risks and issues involved in Safeguarding. The company also recognises that it has a responsibility to protect staff from unfounded allegations of abuse. Steadfast is committed to working with existing local Safeguarding Boards, Health and Social Care partnerships, Police and the Channel Programme to ensure the safeguarding of its learners. Steadfast will work in accordance with the requirements of the Office of the Public Guardian (OPG) and the Mental Capacity Act 2005, supporting the 6 principles of Empowerment, Protection, Prevention, Proportionality, Partnership, and Accountability. The policy applies to all users/all learners and staff of Steadfast Training Ltd who have access to our IT systems, both on the premises and remotely. Any user of Steadfast Training Ltd IT systems must adhere to this policy. The e-Safety Policy (Appendix 2) applies to all who use the internet and forms of electronic communication such as email, mobile phones and social media sites.

Definition

The term “children and young people” refers to “those under the age of 18”, including those who are completing an apprenticeship programme with Steadfast Training Ltd.

In relation to children and young people, Steadfast adopts the definition used in the Children Act 2004, Apprenticeships, Skills, Children and Learning Act 2009 and the Department for Education (DfE) guidance document, Keeping Children Safe in Education 2025, Working Together to Safeguard Children 2023 which defines safeguarding and promoting children and young people’s welfare as:

- protecting children from maltreatment
- preventing impairment of children’s health or development
- ensuring that children are growing up in circumstances consistent with the provision of safe and effective care, and
- taking action to enable all children to have the best outcomes.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

ASCLA (Apprenticeship, Skills, Children & Learning Act 2009) introduced the requirement for an apprentice to be employed under an apprenticeship agreement, this was established to ensure that 16–18-year-olds receive the minimum wage for their age, protected under the working time regulations and work towards a work- based qualification.

Definition of Safeguarding Adults

The term ‘adult at risk’ is used in this policy to replace ‘vulnerable adult’ in accordance with OPG’s statement, that the term ‘vulnerable adult’ may imply that some of the fault for abuse may lie with the victim of abuse.

It is also recognised that some adults are at risk of abuse. Accordingly, our policy and procedures also apply to allegations of abuse and the protection of Vulnerable Groups/Adults Act 2006, the Care Act 2014, Mental Capacity Act 2005, by protection of the Freedoms Act 2012. Guidance on who is an ‘adults at risk’ is taken from ‘No Secrets’ (Department of Health 2000), which defines ‘adults at risk’ as: ‘those adults who are or may be in need of community care services by reason of mental illness or other disability, age or illness’.

The definition of ‘Adults at risk’ (but is not exclusive to) individuals with any of the following:

- Learning Difficulties
- Physical Impairments
- Sensory Impairments
- Mental illness Needs
- Age Related frailty
- Dementia
- Brain Injuries
- Drug or Alcohol Problems
- Domestic Abuse

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

The Mental Capacity Act 2005 (MCA) is a legal framework which protects people who may lack capacity to make decisions for themselves. It also sets out how decisions should be made on their behalf, extra safeguards are needed if the restrictions and restraints used will deprive a person of their liberty. These are called the Deprivation of Liberty Safeguards (DoLS) The presumption is that adults have mental capacity to make informed choices about their safety, how they live their lives and a person's ability to give consent. The Deprivation of Liberty Safeguards (DoLS) are an amendment to the Mental Capacity Act 2005.

Steadfast will adhere to and support all of our learners and employees in accordance with statutory legislation, including '**Clare's Law**' or the **Domestic Violence Disclosure Scheme**.

Definition of Safeguarding Adults

The term 'adult at risk' is used in this policy to replace 'adult at risk' in accordance with OPG's statement, that the term 'adult at risk' may imply that some of the fault for abuse may lie with the victim of abuse.

The Care Act 2014 makes it clear that abuse of adults links to circumstances rather than the characteristics of the people experiencing the harm. Labelling groups of people as inherently 'vulnerable' is seen to be disempowering.

An adult at risk of abuse can be anyone over the age of eighteen, including service users, staff or volunteers. Whilst personal characteristics may make an individual more vulnerable i.e. disability and communication difficulties, it is the situation around an individual which may increase risk or place them at potential risk of harm. It is therefore vital to be open to the possibility that any adult may be at risk and that this can be temporary or on-going depending on the support and protective factors around them.

As stated in the Care Act 2014 "Adult safeguarding" is working with adults with care and support needs to keep them safe from abuse or neglect. It is an important part of what many public services do, and a key responsibility of local authorities.' Safeguarding duties apply to an adult who;

- Has needs for care and support (whether or not the local authority is meeting any of those needs) and;
- Is experiencing, or is at risk of, abuse or neglect; and;
- As a result of those care and support needs is unable to protect themselves from either the risk of, or the experience of, abuse or neglect.

Our policy and procedures also apply to allegations of abuse and the protection of Vulnerable Groups/Adults Act 2006, the Care Act 2014, Mental Capacity Act 2005, by protection of the Freedoms Act 2012.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Prevent Duty

In respect of safeguarding individuals from radicalisation, Steadfast works to the Prevent element of the Government's Counter Terrorism Strategy, and where deemed appropriate seeks external support for learners through referrals to the Channel Programme. This programme aims to work with the individual to address their specific vulnerabilities, prevent them becoming further radicalised and possibly entering the criminal justice system because of their actions. It is recognised that radicalisation can occur to an individual from any section of society and is not particular to any racial, ethnic or social group. It is further recognised that in many instances the process of radicalisation is essentially one of grooming by others.

The risk of radicalisation may be combined with other vulnerabilities. Research shows that indicators of susceptibility to radicalisation can include the following, although it's important to note that there is no specific profile, and this list is not exhaustive:

- **Identity Crisis** - Distance from cultural/religious heritage and discomfort with their place in the society around them;
- **Personal Crisis** - Family tensions; sense of isolation; adolescence; low self-esteem; disassociating from existing friendship group and becoming involved with a new and different group of friends; searching for answers to questions about identity, faith and belonging;
- **Personal Circumstances** - Migration; local community tensions; events affecting country or region of origin; alienation from UK values; having a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy;
- **Unmet Aspirations** - Perceptions of injustice; feeling of failure; rejection of civic life;
- **Criminality** - Experiences of imprisonment; poor resettlement/reintegration; previous involvement with criminal groups.

This Policy applies to all staff, employers and partnership organisations who have a legal responsibility to take seriously any safeguarding issues that come to their attention and follow the procedure as set out in Appendix 1 of this document

- Policy and procedures are issued to all members of staff
- Partners, Subcontractors and Employers will be informed of this Policy and be responsible for reporting any concerns reported to them by contacting the Designated Person.
- All learners are referred to this Policy at their induction.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Accountability and Responsibility Duty to Report

This Policy applies to all staff, employers and partnership organisations who have a legal responsibility to take seriously any safeguarding issues that come to their attention and follow the procedure as set out in Appendix 1 of this document

- Policy and procedures are issued to all members of staff
- Partners, subcontractors and Employers will be informed of this Policy and be responsible for reporting any concerns reported to them by contacting the Designated Person.
- All learners are referred to this Policy at their induction

Key staff with designated safeguarding responsibilities includes:

- **Managing Director:** To ensure the promotion of ALL Safeguarding throughout the organisation and all partnerships.
- **Designated person:** To record, document and act appropriately to ALL safeguarding disclosures
- **Designated officer:** To record and instigate an investigation into the Safeguarding incident or concern. To document and disclose timely to the Local Multidisciplinary team.

Steadfast has three Safeguarding appointed persons from the management team who are accountable to the Managing Director. Incidents or concerns are reported at local level to the appointed persons and escalated to the Director. The Safeguarding Appointed Persons are responsible for monitoring and managing incidents or concerns and liaising with the respective safeguarding agencies. The Safeguarding Appointed Person will produce an annual report on safeguarding issues raised.

Training

The company has a duty to promote safeguarding issues and measures to staff and ensure they:

Analyse their own practice against established good practice, and assess risk to ensure their practice is likely to protect them from false allegations.

- Recognise their responsibilities and report any concerns about suspected poor practice or possible abuse (Code of Conduct)
- Follow the guidelines provided for all staff, related partners and employers
- All staff will undertake annual training on safeguarding to raise awareness of current issues and legislation.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

- The Safeguarding Appointed Person will attend the recommended designated person Training every 2 years.

Employees, who are responsible for recruitment of staff, have also taken further safeguarding training 'safer recruitment' to ensure that all policies, procedures and pre- appointment checks are completed safely and accurately.

Disclosure Barring Service

The company recognises it has a responsibility to ensure safe recruitment and employment practices. Steadfast outsource the service of a registered company who complete DBS checks on new and existing staff who frequently or intensively work with children, young people and adults at risk in training, supervision advice and guidance.

Review

The Managing Director will review the Safeguarding Policy and associated relevant documents annually.

Relevant Documents

This policy and procedure should be read in conjunction with the Code of Conduct for Staff, Safeguarding Flowchart and the Safeguarding leaflets issued to all learners at induction.

All staff should keep a copy of Appendix 1 – reporting guide

A very useful reference guide for all staff, partners and employers is Safer Practice, Safer Learning from the National Institute of Adult and Continuing Education (NIACE)
<https://www.excellencegateway.org.uk/content/import-pdf4619>

Jason Parnell

CEO

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

PROCEDURE FOR REPORTING CASES OF SUSPECTED ABUSE INVOLVING CHILDREN/YOUNG PEOPLE OR ADULTS AT RISK.

1. THE DUTY TO REPORT

- 1.1 **WE ALL** have a legal duty to report cases of suspected abuse. If you, have concerns that a child/young person or adults at risk who have been mistreated or abused or at risk of being radicalised, you **MUST** report this, see (F1057 Adult Safeguarding Incident Reporting Form) which must go directly to the Designated Appointed Person as soon as possible

TYPES OF ABUSE

Categories of Abuse and neglect can take many forms. Individuals should not be constrained in their view of what constitutes abuse or neglect and should always consider the circumstances of the individual case. The Care Act 2014 highlights 10 categories of abuse.

Physical abuse may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning or otherwise causing physical harm. Physical injury may occur as a result of injury inflicted by a family member, including a brother or sister, or by another person, or an injury sustained accidentally but as a result of neglect. Physical harm may also be caused when a parent or carer feigns the symptoms of, or deliberately causes ill health to a child whom they are looking after. This situation is commonly described using terms such as fabricated or induced illness by proxy, or Munchausen Syndrome by Proxy.

Bullying can also be a form of physical and emotional abuse. However, it is more often between peers and needs to be dealt with locally by personal Trainers and Tutors with the assistance of Designated Appointed Person, with cases reported as per Steadfast Anti-Harassment & Bullying Policy.

Psychological/Emotional Abuse is the persistent emotional ill-treatment of a person such as to cause severe and persistent adverse effects on him or her emotional development. This may include threats of harm or abandonment, deprivation of contact, humiliation, blaming, controlling, intimidation, coercion, harassment, verbal abuse, isolation, or withdrawal from services or supportive networks. It may also involve conveying to that child or person that they are worthless or unloved, inadequate or valued only in so far as they meet the needs of another person. It may feature age or developmentally inappropriate expectations being imposed on the child or person concerned. It may involve causing that child or person to feel frightened or in danger, or exploitation or corruption. Emotional and other forms of abuse may occur as a result of domestic abuse. Some level of emotional abuse is involved in all types of ill-treatment or abuse, though it may occur alone.

Domestic abuse is classed as any incident or pattern of incidents of controlling,

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality. This can encompass but is not limited to Psychological, Physical, Sexual, Economical and Emotional abuse, it also can include “honour” based violence, forced marriage and female genital mutilation (FGM). Domestic Abuse is not confined to one gender or ethnic group.

Sexual abuse involves forcing or enticing a child or adult at risk to take part in sexual activities, whether they are aware of what is happening or not. The activities may involve physical contact, including penetrative or non-penetrative acts. They may include non-contact activity such as involving children or adult at risks in looking at, or in the production of, pornographic material or watching sexual activities, or encouraging them to behave in sexually inappropriate ways. Sexual abuse may also take place through the inappropriate use of cameras and phone images.

Neglect and act of omission is the persistent failure to meet a child or adult at risk’s basic physical and/or psychological needs, likely to result in the serious impairment of his or her health or development. It may involve a parent or carer ignoring medical or physical care needs, failure to provide access to appropriate health, care and support or educational services, the withholding of the necessities of life, such as medication, adequate nutrition and heating.

Financial or material abuse [economical abuse] is defined as the misappropriation of money or assets; transactions to which the person could not consent or which were invalidated by intimidation or deception; or, the misuse of assets. Examples include misuse of benefits, denying access to money, not spending allowances on the individual, and unreasonable restriction on a person’s right to control over their lives to the best of their ability. This includes theft, fraud, internet scamming, and coercion in relation to an adult’s financial affairs or arrangements.

Discriminatory abuse is defined as any form of abuse based on a person’s age, race, gender - or any of the protected characteristics stated in the Equality Act 2010.

Organisational/Institutional abuse includes neglect and poor care practice within an institution or specific care setting, such as a hospital or care home, or in relation to care provided in one’s own home.

Institutional abuse is defined as incidents of poor professional practice or neglect, and inflexible services. This can be through neglect or poor professional practice because of the structure, policies, processes and practices within an organisation. Organisational abuse may take the form of physical, financial, emotional abuse, inappropriate use of power and neglect.

Modern Slavery encompasses slavery, human trafficking, forced labour, forced marriage and domestic servitude.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Self Neglect covers a range of behaviours related to neglecting to care for one's own personal hygiene, health or surroundings. An example of this behaviour is hoarding. The Care Act 2014 states A decision on whether a response is required under safeguarding will depend on the adult's ability to protect themselves by controlling their own behaviour.

There are four additional types of harm that are not included in The Care Act, but they are also relevant to safeguarding adults. These are;

Cyber Bullying Cyber-Bullying is a type of bullying which can involve the victim being harassed, humiliated, embarrassed, or otherwise targeted via the internet, social media or by mobile phone. It includes various different types of bullying, including racist bullying, homophobic bullying, or bullying related to special education needs and disabilities.

Mate-Crime A "mate crime" is when "vulnerable people are befriended by members of the community who go on to exploit and take advantage of them" (The Safety Net Project, ARC). This can lead to, but not limited to, people losing their independence, financial, physical, and sexual abuse. Mate Crime can also lead to '**Cuckooing**' which is a practice where people take over a person's home and use the property to facilitate exploitation.

Forced Marriage. This is a term used to describe a marriage in which one or both of the parties are married without their consent or against their will, or coercion or pressure may be a factor This does not include arranged marriages where both parties consent to enter the marriage. The Anti-Social Behaviour, Crime and Policing Act 2014 made it a criminal offence to force someone to marry.

Radicalisation is the process through which a person comes to support or be involved in extremist ideologies. It can result in a person becoming drawn into terrorism and is in itself a form of harm. The process of radicalisation is different for every individual and can take place over an extended period or within a very short time frame.

POSSIBLE SIGNS OF RADICALISATION CAN INCLUDE:

Radicalisation can be difficult to spot, but possible signs that could indicate radicalisation include:

- Behaviour change
- Changing social circle
- Isolating from family and friends
- Speaking in a scripted manner
- Unwillingness or inability to discuss views
- Sudden disrespect towards others

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

- Increased anger levels
- Heightened secrecy, especially online
- Accessing extremist material online
- Using extremist or hate terms to exclude or incite violence
- Creating violent extremist messages through writing or artwork
- Growing extreme views towards a specific group or government policy
- Decreased tolerance for moderate views
- Expressing desire/intent to participate in or support extremist activity
- Downloading, viewing, or sharing extremist propaganda
- Becoming fixated on one ideology
- Changes in appearance and declining health (including mental illness)

2. WHAT TO DO IF YOU NOTICE ABUSE/SIGNS OF RADICALISATION

2.1 You may become aware of potential abuse in three ways:

2.11 you may observe signs in a student that lead you to suspect that they have been physically, emotionally, or sexually abused, or suffer severe neglect, or are becoming radicalised; or in addition in the case of an adult at risk, they may be experiencing financial, discriminatory, or institutional abuse.

2.12 In addition to these a person may be being abused by virtue of their race, gender, age, disability, or sexual orientation which would indicate discriminatory abuse. Similarly, any of the examples listed may be an indication of institutional abuse if the individual is in receipt of organised care.

2.13 the students themselves may disclose to you that they have been abused.

2.2 If a student discloses to you that they (or indeed another child/young person or adult at risk) have been, or are being abused/radicalised

DO

- **Do** listen very carefully to what they tell you.
- **Do** take what is said seriously and accept what you are told.
- **Do** stay calm and reassure the student that they have done the right thing in talking to you.
- **Do** write down as soon as you can exactly what you have been told.
- **Do** tell them that you must pass this information on but that only those that need to know will be told. Tell them to whom you will report the matter.
- **Do** preserve any evidence, taking pictures if possible and

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

appropriate.

DO NOT

- **Do not** panic.
- **Do not** promise to keep things secret. You have a duty to refer a child/young person or adult who is at risk.
- **Do not** lie or say that everything will be fine now that they have told.
- **Do not** criticise the abuser, especially if it is a parent/carer
- **Do not** ask lots of detailed or leading questions such as: 'What did he do next?' Instead, ask open questions such as: 'Anything else to tell me? 'Yes', or 'And...?'. Do not press for answers the student is unwilling to give.
- **Do not** dispose of any evidence or allow the individual to wash themselves.

It is important that the person to whom disclosure is made **does not investigate** or question the person concerned except to clarify what they have heard. This is particularly important in cases of sexual abuse.

- 2.3 It is very important to record, as accurately as possible, what was said to you when you received the disclosure of abuse/radicalisation. Clearly all written records should be handled confidentially.
- 2.4 **You must inform the designated person immediately** if you have concerns that a child/young person or adult at risk has been, or is, being abused / radicalised. They should be informed in person, or by telephone or (in extreme circumstances) by email.
- 2.5 If, for any reason, you are unable to contact the designated person (for example in the evening) and the matter is urgent, then contact the Local Authority or the police directly and report the matter to the Curriculum Lead at next available opportunity.
- 2.6 **In all cases, if you are concerned, the rule is to pass this on quickly** and to seek help and further support, rather than to worry alone or to do nothing.

3. THE ROLE OF THE DESIGNATED TEAM

- 3.1 When a member of staff refers a case of suspected abuse to a member of the Designated Team, The Lead DAP will decide whether or not the situation should be referred to the Local Authority or the police, or whether some other course of action is more appropriate. If they consider that abuse may have taken place, or that a child/young person or adult

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

at risk, is at risk of abuse/radicalisation, they will formally notify the Local Authority or police about this. Most local authorities and safeguarding teams require an **Adult Alert Form** completed initially (located on the relevant website), containing all relevant, factual and accurate details. At this point they will take responsibility making further investigations.

- 3.2 At this point the Local Authority take over responsibility for the issue. If they decide that there are serious concerns, they will initiate a formal assessment and, where circumstances warrant it, involve the police.
- 3.3 A confidential record will be kept of all cases referred to the Designated Team, including details of cases referred to the Local Authority or the police. These records will be kept securely via a restricted file on Steadfast "S" drive system, with any paper information held securely by the HR – Finance Controller.
- 3.4 Disclosure of or being the subject of abuse is obviously a very difficult and distressing time for the student, who will be made aware of the support available to them and helped to initiate contact with this support if so desired.

Involvement in cases of suspected abuse can be personally disturbing and distressing. Although the individuals involved in taking the disclosure may feel a need to talk about it with someone – a colleague, a friend, a partner – they should avoid this in order to respect the confidentiality of the student concerned and only talk to a member of the designated team.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

External Contact Numbers

Safeguarding Adult Teams:	FE/HE Prevent Co-ordinators:										
<u>Lincolnshire:</u> Adults safeguarding - 01522 782155 (Monday to Friday, 8.00am to 6.00pm) or 01522 782333 (outside office hours) <u>Leicester:</u> Telephone: 0116 454 1004 (Monday to Thursday 8.30am to 5pm, Friday 8.30am to 4.30pm) Emergency number: 0116 255 1606 (6pm to 8am) <u>Northamptonshire:</u> Customer Service Centre on 0300 126 1000, option 2. The Emergency Duty Team can be contacted outside office hours on 01604 626938. <u>Derbyshire:</u> derbyshiresab@derbyshire.gov.uk Telephone: 01629 533190 <u>Staffordshire & Stoke on Trent:</u> SSASPB.admin@staffordshire.gov.uk If the adult lives in Stoke: Telephone: 0800 561 0015 at any time	<u>East Midlands:</u> Sam Slack Sam.slack@derby.gov.uk Mobile: 07384 452156 <u>Prevent Referrals:</u> <table> <tr> <td>Nottinghamshire</td><td></td></tr> <tr> <td>Lincolnshire</td><td></td></tr> <tr> <td>Derbyshire</td><td></td></tr> <tr> <td>Northamptonshire</td><td></td></tr> <tr> <td>Leicestershire</td><td></td></tr> </table>	Nottinghamshire		Lincolnshire		Derbyshire		Northamptonshire		Leicestershire	
Nottinghamshire											
Lincolnshire											
Derbyshire											
Northamptonshire											
Leicestershire											

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

If the adult lives in Staffordshire:

Telephone: 0345 604 2719 Monday to Thursday 8:30am to 5pm, Fridays 8:30am to 4:30pm, excluding Bank Holidays

0345 604 2886 at any other time

Essex:

essexsocialcare@essex.gcsx.gov.uk

0345 603 760

Bedfordshire:

Adult.protection@bedford.gov.uk

01234 276222

For after-hours emergencies only contact Tel: 0300 300 8123

Hertfordshire:

Adult.safeguarding@hertscc.gcsx.gov.uk

Telephone: 0300 123 4042

North East: Gateshead

adultsocialcaredirect@gov.uk

0191 433 7033

North East: Newcastle: 01912 788

3377

Suffolk: 0808 800 4005

Norfolk: 0344 800 8020

Cambridgeshire:

referral.centre

adults@cambridgeshire.gov.uk

0345 045 5202

Peterborough

adultsocialcare@peterborough.gov.uk

01733 747474

North Yorkshire: 01609 780780

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Appendix 1 - Reporting guide handout

This procedure **must** be followed whenever any member of staff or related partner / employer hears an allegation from a child or adult at risk, that abuse has, or may have, occurred or where there is a significant concern that a child or adult at risk, may be abused/radicalised:

RECEIVE

What is said

- Accept what you are told – you do not need to decide whether or not it is true
- Listen without displaying shock or disbelief.

REASSURE

- The learner/member of staff
- Acknowledge their courage in telling
- Do not promise confidentiality
- Remind them they are not to blame – avoid criticising the alleged perpetrator
- Do not promise that “everything will be alright now” (it might not be)

REACT

- Respond to the learner/member of staff but do not interrogate
- Avoid leading questions but ask open ended ones
- Clarify anything you do not understand
- **Explain what you will do next, i.e. inform a Designated Person**

RECORD

- Make notes as soon as possible – during the interview if you can.
Include: time, date, place, the learner/staff member’s own words – do not assume – ask,
e.g. “Please tell me what xxxxx means”.
- Describe observable behaviour and appearance
- Cross out mistakes – do not use Tippex
- Do not destroy your original notes – they may be needed later on and must be given to the Designated Person.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

SUPPORT

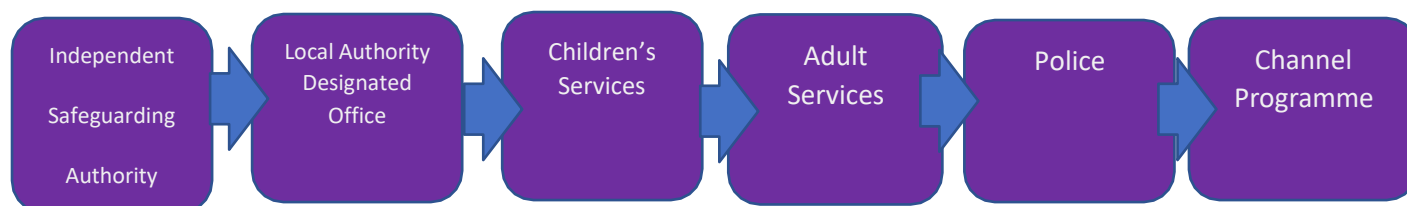
- Consider what support is needed for the learner/staff member – you may need to give them a lot of your time to ensure they feel reassured and supported.
- Ensure you are supported – such interviews can be extremely stressful and time consuming
- Once reported to them, the Designated Person will take responsibility for the matter and will take the necessary actions. However, if you have questions or need additional support then do ask.

Contact Information:

Safeguarding Leads:
Robert Wright: Robert.Wright@steadfasttraining.co.uk Telephone: 0845 223 2401 Mobile: 07985338185 Alison Law Alison.law@steadfasttraining.co.uk Telephone: 0845 223 2401 Mobile: 07720092609 Chloe Robinson Chloe.Robinson@steadfasttraining.co.uk Mobile: 07985338116

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Safeguarding/PREVENT FLOWCHART



Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Appendix 2

E-Safety policy

Roles and Responsibilities

There are clear lines of responsibility for e-safety within the company. The first point of contact should be Head of Quality and Curriculum. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All Trainers and Tutors are required to offer guidance on e-safety to their learners and to read through and report incidents in line with the policy. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be the Head of Quality and Curriculum. All parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Safeguarding Officer may be asked to intervene with appropriate additional support from external agencies.

e-Safety Officer/Safeguarding Officer

The Safeguarding Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to complete, review, and update the e-Safety Policy, deliver staff development and training, record incidents, report any developments and incidents to the SMT and liaise with the local authority and external agencies to promote e-safety.

Learner:

Learners are responsible for using Steadfast Training Ltd IT systems and mobile devices in accordance with the company requirements. Learners must always act safely and responsibly when using the internet and/or mobile technologies. They are responsible for attending e-safety lessons as part of the curriculum and are expected to know and act in line with other relevant company policies e.g. mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the company.

Staff:

All staff are responsible for using Steadfast Training Ltd IT systems and mobile devices in accordance with the company Acceptable Use Policies No.114 & 115. Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times.

All staff should apply relevant company policies and understand the safeguarding incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the Designated Safeguarding Officer and/or line manager without delay.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Security

The company will do all that it can to make sure the company network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access of company systems and information. Digital communications, including email and internet postings, over the company network, will be monitored in line with the IT, Computer Usage Policy No114.

Artificial Intelligence (AI) Safeguarding and Learner Protection Considerations

As Artificial Intelligence (AI) tools become increasingly prevalent across education, employment, and everyday life, it is essential that their use within the Independent Training Provider (ITP) is consistent with our safeguarding and learner protection duties. This appendix sets out the principles and procedures for managing AI-related safeguarding risks in line with Keeping Children Safe in Education (KCSIE), Working Together to Safeguard Children, and the ITP's broader safeguarding and Prevent responsibilities.

AI and the Safeguarding Context

AI technologies — including chatbots, image generators, recommendation systems, and predictive tools can bring significant educational and operational benefits. However, they also introduce new safeguarding, ethical, and data protection challenges.

The ITP recognises that AI tools can:

- Influence behaviour, opinions, and decision-making.
- Generate inappropriate, misleading, or harmful content.
- Be misused — deliberately or unintentionally — to bypass safety and filtering systems.

All use of AI within the ITP must therefore be guided by a safeguarding-first approach, ensuring that the wellbeing and safety of all learners — including those under 18 and vulnerable adults — are prioritised.

Key Safeguarding Controls

a. Age- and Role-Appropriate Access

- Learners will not be provided with access to any AI platform that carries an age restriction higher than their chronological age.
- Tutors, assessors, and support staff must verify the age and content suitability of any AI-enabled resource or application used in training, assessment, or support.

b. Supervised and Structured Use

- AI tools may only be used for approved curriculum or training purposes.
- Staff must ensure that learners understand both the advantages and limitations of AI, particularly when completing self-directed or work-based tasks.
- Unfiltered or unsupervised use of generative AI is not permitted on ITP systems or devices.

c. No Sharing of Personal or Sensitive Information

- Learners must never input personal, identifiable, or work-related data into AI systems.
- Staff must not upload, describe, or reference any learner's personal, safeguarding, or employer-related information within AI tools.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

- AI systems must never be used to record, analyse, or manage safeguarding information.

3. Emerging Safeguarding Risks

The ITP recognises the following as key risk areas associated with the use of AI:

- Exposure to inappropriate or harmful content — AI tools may generate or reproduce explicit, violent, or distressing material, even unintentionally.
- Misinformation and bias — AI systems can present false, misleading, or discriminatory information.
- Impersonation and identity misuse — AI-generated media, including deepfakes, can mimic real individuals.
- Exploitation and manipulation — learners may be exposed to AI-assisted scams, radicalisation, grooming, or coercive behaviour online.
- Psychological and emotional impact — over-reliance on, or negative interaction with, AI tools may affect confidence, mental health, or perceptions of self and others.

Staff Responsibilities and Training

All staff are required to:

- Remain vigilant for signs that learners may be misusing AI or have encountered harmful content.
- Integrate AI safety and ethics into digital literacy, Prevent, and safeguarding discussions.
- Report any AI-related concerns through established safeguarding procedures without delay.
- Avoid using AI to communicate directly with learners or to produce unreviewed teaching materials.
- Engage in relevant CPD to remain informed about emerging digital risks.

Learner Education and Awareness

AI awareness will be embedded within Steadfast Training Ltd digital safety and Prevent curriculum.

Learners will be supported to understand:

- What AI is, how it operates, and its limitations.
- How to identify and critically evaluate AI-generated content.
- Why personal or identifying information must never be shared with AI or online systems.
- How to seek help and report concerns relating to AI-generated or online content.

Monitoring, Reporting, and Response

- All use of the internet is monitored — including attempts to access AI platforms — through the organisation's approved monitoring software
- Any safeguarding concern involving AI will be managed in line with the Safeguarding and Child/Adult Protection Policy.
- Where concerns involve use of AI outside of training sessions, the Designated Safeguarding Lead (DSL) will liaise with employers, parents or carers (where applicable), and relevant external agencies such as the Police, CEOP, or Prevent partners.

Oversight, Governance, and Review

- The Designated Safeguarding Lead (DSL), in partnership with the Online Safety Lead and Data Protection Officer (DPO), will oversee all AI-related safeguarding and data protection matters.
- AI-related risks will be reviewed annually as part of the safeguarding audit and policy review process — or sooner if technology changes or incidents arise.
- All staff and learners will be informed of new threats, guidance, or operational changes relating to AI use.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

Behaviour

Steadfast Training Ltd will ensure that all users of technologies adhere to the standard of behaviour as set out in the IT, Computer Usage Policy No 114.

The company will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the company and staff disciplinary codes.

Where conduct is found to be unacceptable, the company will deal with the matter internally. Where conduct is considered illegal, the company will report the matter to the police.

Communications

Steadfast Training Ltd requires all users of IT to adhere to Use of Internet, Email & Social Media Policy No. 115 which states clearly when email, mobile phones, social media sites, games consoles, chat rooms, video conferencing and web cameras may be used during the day. All sensitive and personal data shared via email both internally and externally, will be sent via secure technology, for example Encryptmail or similar secure encryption

Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g., images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

All learners and staff should receive information on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves, or others are posted onto social networking sites.

This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

Personal Information

Personal information is information about a particular living person. Steadfast Training Ltd collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The company will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner/parent/carer. No personal information can be posted to the company website/without the permission of the Designated Safeguarding Officer unless it is in line with our Data Protection Policy No 112. Only names and work email addresses of (senior) staff will appear on the company website/no

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026

staff/no learners' personal information will be available on the website without consent.

Staff must keep learners' personal information safe and secure at all times. No personal information of individuals is permitted offsite unless the member of staff has the permission of Designated Safeguarding Officer. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection and Confidentiality policy No 112.

Education and Training

With the current unlimited nature of internet access, it is impossible for the company to eliminate all risks for staff and learners. It is our view therefore, that the company should support staff and learners stay e-safe through regular training and education.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Staff will take part in e-safety training before beginning a new company year. This will be led by the Designated Safeguarding Officer and will take the format of a workshop, allowing tutors' hands-on experience. Further resources of useful guidance and information will be issued to all staff following the session. Each member of staff must record the date of the training attended on their CPD calendar.

Incidents and Response

Where an e-safety incident is reported to the company this matter will be dealt with very seriously. The company will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or to the company Designated Safeguarding Officer. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the company will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Version	Owner	Author	Signature	Date	Changes made	Next Review
10	DSL	DSL Team		November 2025	Updated to reflect AI	November 2026