



SAFEGUARDING & CHILD PROTECTION POLICY

Policy Owner: Head Office

Designated Safeguarding Lead (DSL): Appointed by the Grand Council

Deputy DSL: Appointed by the Grand Council

Governance Oversight: Grand Council

Applies to:

All staff, examiners, Teacher Members, centres, contractors, consultants, volunteers, trustees, committee members, partners, and any individual acting on behalf of I-PATH

Review Frequency: Annual minimum and immediately following any safeguarding incident, legislative change, or regulatory direction

Last Reviewed: 9th February 2026

1. Safeguarding Statement (Non-Negotiable)

International Performing Arts & Theatre Limited (I-PATH) is unequivocally committed to safeguarding and promoting the welfare of all children, young people, and vulnerable adults.

Safeguarding is not a supporting function - it is a core organisational duty.

No operational, reputational, commercial, or assessment consideration shall ever override safeguarding.

I-PATH operates a zero-tolerance approach to abuse, neglect, exploitation, unsafe practice, or safeguarding complacency.

2. Why Safeguarding Is Critical in an Exam Board Context

I-PATH recognises that safeguarding risks in an examining and assessment environment differ materially from those in schools.

Specific risks include:

- short-term but intense contact with children
- one-off or infrequent supervision
- high-pressure performance environments
- power imbalance between examiners and candidates
- online and recorded assessments
- third-party venues beyond I-PATH's direct control
- reliance on centres and teachers for supervision

This policy is therefore explicitly designed for an exam board, not a school.

3. Legal, Statutory and Regulatory Framework

This policy complies with and is informed by:

UK Legislation

- Children Act 1989
- Children Act 2004
- Children and Families Act 2014
- Sexual Offences Act 2003
- Safeguarding Vulnerable Groups Act 2006
- Protection of Freedoms Act 2012
- Equality Act 2010
- Human Rights Act 1998
- UK GDPR & Data Protection Act 2018

Statutory Guidance

- *Keeping Children Safe in Education* (DfE)
- *Working Together to Safeguard Children*
- *What to do if you're worried a child is being abused*

Regulatory Expectations

- Ofqual Handbook – Conditions relating to:
 - organisational capability
 - learner protection
 - governance and risk
 - public confidence in qualifications

4. Definitions (Precise and Enforceable)

Child: Any person under the age of 18.

Safeguarding: Protecting children from maltreatment, preventing impairment of health or development, ensuring safe and effective care, and taking action to enable best outcomes.

Child Protection: Specific action taken to protect a child who is suffering, or is likely to suffer, significant harm.

Vulnerable Adult: An adult who may be unable to protect themselves due to disability, illness, age, mental health, or situational vulnerability.

5. Core Safeguarding Principles

I-PATH safeguarding practice is founded on:

1. The welfare of the child is paramount
2. Safeguarding is everyone's responsibility
3. Early action prevents escalation
4. Professional curiosity is required
5. Silence, minimisation and delay are safeguarding failures
6. Safeguarding overrides confidentiality
7. Safeguarding overrides customer service
8. Safeguarding overrides assessment delivery

6. Governance, Accountability and Authority

6.1 Grand Council

The Grand Council:

- holds ultimate safeguarding accountability
- ensures sufficient resources are allocated
- receives safeguarding reports
- challenges safeguarding performance
- authorises safeguarding policy

6.2 Designated Safeguarding Lead (DSL)

The DSL:

- has absolute authority on safeguarding matters
- receives all safeguarding concerns
- determines thresholds for action
- liaises with statutory agencies
- maintains safeguarding records
- reports directly to governance

The DSL does not require permission from operational teams to escalate concerns.

A trained Deputy DSL ensures continuity at all times.

7. Roles and Responsibilities

All Adults Must:

- understand safeguarding indicators
- remain alert to concerns

- act immediately on suspicion
- report, not investigate
- record accurately

Failure to act is itself a safeguarding breach.

8. Safer Recruitment & Ongoing Suitability

I-PATH operates robust safer recruitment including:

- enhanced DBS with Update Service
- identity verification
- qualification verification
- reference scrutiny
- safeguarding-focused interviews
- ongoing suitability monitoring

Safeguarding suitability is continuous, not a one-off check.

Refer to our Safer Recruitment Policy.

9. Safe Staffing & Supervision

Mandatory rules:

- Minimum two-adult rule at all times
- No lone working with children
- Staffing ratios determined by risk
- Examiners empowered to halt activity

Breaches trigger immediate escalation.

Refer to our Safe Staffing Policy.

For all Face-to-Face (F2F) and Live Video Examinations (LVE), I-PATH requires a minimum two-adult presence, consisting of the examiner and an additional responsible adult aged 18+. Detailed requirements are set out in the Two-Adult Presence Policy. Failure to comply constitutes a safeguarding breach and may result in suspension or termination of examination activity.

10. Professional Boundaries (Zero Tolerance)

Prohibited behaviours include:

- private messaging learners
- social media contact
- personal phone numbers

- unsupervised 1:1 contact
- gifts or favours
- sexualised language or behaviour
- physical contact beyond necessity

Intent is irrelevant - impact and risk are decisive.

11. Categories of Abuse

Including but not limited to:

| | |
|-------------------------------|---|
| <p>Physical abuse</p> | <p>Physical abuse occurs when an adult or another person deliberately causes physical harm to a child or young person, or fails to prevent physical harm. This may involve actions such as hitting, slapping, punching, shaking, throwing, poisoning, burning, scalding, biting, suffocating or drowning.</p> <p>Physical abuse also includes:</p> <ul style="list-style-type: none"> • the deliberate administration of alcohol, drugs or other harmful substances to a child or young person, or • knowingly allowing a child or young person to consume substances that are inappropriate, unsafe or unlawful for their age. <p>Physical abuse may also take the form of fabricated or induced illness (FII), previously known as <i>Munchausen syndrome by proxy</i>, where a parent or carer:</p> <ul style="list-style-type: none"> • fabricates, exaggerates or falsifies symptoms of illness in a child, or • deliberately induces illness or injury in a child in their care, resulting in unnecessary medical intervention or harm. |
| <p>Emotional abuse</p> | <p>Emotional abuse is the persistent emotional maltreatment of a child or young person that has, or is likely to have, a serious and lasting adverse effect on their emotional development, wellbeing or sense of self-worth.</p> <p>Emotional abuse may include, but is not limited to:</p> <ul style="list-style-type: none"> • repeatedly telling a child or young person that they are worthless, useless, unloved, inadequate or only valued in so far as they meet the needs of another person • imposing developmentally inappropriate expectations, demands or responsibilities • consistently criticising, belittling, humiliating or rejecting a child or young person • making a child or young person feel frightened, threatened or unsafe, including through shouting, intimidation, threats or persistent verbal aggression • exposing a child or young person to behaviour that causes them to become withdrawn, anxious, distressed or fearful. |

| | |
|----------------------------|--|
| | <p>In a performing arts and assessment context, emotional abuse may occur where a child or young person is:</p> <ul style="list-style-type: none"> • subjected to persistent or excessive criticism that is not constructive or proportionate • repeatedly given negative feedback without support, balance or developmental guidance • expected or pressured to perform beyond their physical, emotional or developmental capability • shamed, ridiculed or demeaned in relation to performance, appearance, ability or progress • subjected to name-calling, bullying or demeaning language, whether by adults or peers. <p>Emotional abuse may occur both in isolation and alongside other forms of abuse. The absence of physical harm does not lessen the seriousness of emotional abuse.</p> |
| <p>Sexual abuse</p> | <p>Sexual abuse involves forcing, coercing or enticing a child or young person to take part in any sexual activity, whether or not the child understands what is happening, and regardless of whether violence is used.</p> <p>Sexual abuse may involve physical contact, including:</p> <ul style="list-style-type: none"> • assault by penetration (such as rape or oral sex), or • non-penetrative acts including masturbation, kissing, rubbing or inappropriate touching, whether over or under clothing. <p>Sexual abuse may also involve non-contact activities, including:</p> <ul style="list-style-type: none"> • involving a child or young person in the production, viewing or sharing of sexual images or videos • exposing a child to sexual acts or sexualised behaviour • encouraging or pressuring a child to behave in sexually inappropriate ways • grooming, including online grooming, in preparation for abuse, exploitation or sexual activity. <p>Sexual abuse can occur in person or online, and may be carried out by:</p> <ul style="list-style-type: none"> • adults of any gender, or • other children or young people. <p>Sexual abuse can occur without physical contact, without the use of force, and without the child’s immediate awareness. The absence of resistance, injury or disclosure does not indicate consent and does not reduce the seriousness of the abuse.</p> |

| | |
|----------------------------------|---|
| <p>Neglect</p> | <p>Neglect occurs when a parent, carer or other responsible adult persistently or severely fails to meet a child or young person’s basic physical and/or psychological needs, resulting in, or likely to result in, serious impairment of the child’s health, safety, wellbeing or development.</p> <p>Neglect may include, but is not limited to:</p> <ul style="list-style-type: none"> • failure to provide adequate food, clothing, shelter or supervision • failure to protect a child or young person from physical harm, danger or foreseeable risk • failure to ensure access to appropriate medical care, treatment or therapeutic support • failure to meet a child or young person’s emotional and psychological needs, including consistent care, nurture and reassurance • persistent emotional unavailability, rejection or withdrawal of affection, love or attention where this has a damaging impact on the child’s wellbeing. <p>In a performing arts, teaching or assessment context, neglect may occur where a child or young person is:</p> <ul style="list-style-type: none"> • not kept physically safe during lessons, rehearsals, performances or examinations • exposed to unsafe environmental conditions, including excessive cold, heat, fatigue or dehydration • required to continue activity despite injury, illness, exhaustion or distress • placed at unnecessary risk of harm through inadequate supervision, poor risk management or unsafe practice. <p>Neglect may be a single serious incident or a pattern of ongoing behaviour and can be just as harmful as other forms of abuse.</p> |
| <p>Peer-on-peer abuse</p> | <p>Peer-on-peer abuse refers to any form of abuse that occurs between children or young people, rather than being perpetrated by an adult. It can take place inside or outside educational, performance or assessment settings, and may occur in person or online.</p> <p>Peer-on-peer abuse may include, but is not limited to:</p> <ul style="list-style-type: none"> • physical abuse, such as hitting, kicking, biting or causing injury • emotional or psychological abuse, including bullying, intimidation, humiliation or coercive behaviour • sexual abuse or sexual harassment, including unwanted sexual touching, sexualised language, sharing sexual images, pressuring others into sexual activity, or sexual exploitation • online abuse, including cyberbullying, online harassment, coercion or exploitation through digital platforms |

| | |
|----------------------------|---|
| | <ul style="list-style-type: none"> • harmful sexual behaviour, including behaviour that is developmentally inappropriate or abusive • discriminatory abuse, including abuse motivated by race, gender, disability, sexual orientation, religion or other protected characteristics. <p>Peer-on-peer abuse can be serious and harmful, and should never be dismissed as “banter”, “initiation”, “part of growing up” or “performance culture”. All instances must be taken seriously, investigated appropriately and addressed in line with safeguarding procedures.</p> <p>A child or young person who engages in peer-on-peer abuse may also be a victim of abuse and requires safeguarding support. The welfare and safety of all children involved must remain the primary concern.</p> |
| <p>Online abuse</p> | <p>Online abuse refers to any form of abuse that occurs through, or is facilitated by, digital technology, including the internet, social media platforms, messaging services, gaming environments, livestreaming tools and other online or electronic communication methods.</p> <p>Online abuse may include, but is not limited to:</p> <ul style="list-style-type: none"> • cyberbullying, including harassment, intimidation, humiliation or threats • online sexual abuse and exploitation, including grooming, coercion, sexual harassment or pressure to engage in sexual activity • the creation, sharing or possession of sexual images or videos of children and young people • exposure to inappropriate, harmful or distressing content • coercive or controlling behaviour, including blackmail or manipulation • impersonation, identity abuse or misuse of images or recordings • abuse facilitated through live video, recorded video or online assessment platforms. <p>Online abuse can occur at any time, across multiple platforms, and may be perpetrated by:</p> <ul style="list-style-type: none"> • adults, or • other children or young people. <p>Online abuse may be hidden from adults, may occur alongside face-to-face abuse, and can have serious and lasting impacts on a child or young person’s wellbeing, safety and mental health.</p> <p>All concerns relating to online abuse must be taken seriously and responded to in line with safeguarding procedures, regardless of whether the abuse occurs on I-PATH systems or external platforms.</p> |
| <p>Grooming</p> | <p>Grooming is a process by which an individual builds a relationship, trust or emotional connection with a child or young person in order to manipulate, exploit or abuse them, or to prepare them for future abuse or exploitation.</p> |

| | |
|---------------------|---|
| | <p>Grooming may involve:</p> <ul style="list-style-type: none"> • giving special attention, gifts or favours • offering praise, flattery or emotional support in order to create dependency • isolating a child or young person from peers, family or trusted adults • testing boundaries and normalising inappropriate behaviour • using secrecy, threats, guilt or emotional manipulation • desensitising a child or young person to sexualised language, behaviour or content. <p>Grooming can occur:</p> <ul style="list-style-type: none"> • online or in person • over a short or extended period of time • without the child or young person recognising it as abuse. <p>Grooming may be carried out by:</p> <ul style="list-style-type: none"> • adults, or • other children or young people. <p>The intention behind grooming is to reduce resistance, increase compliance and gain control, and it may lead to sexual abuse, exploitation, emotional abuse, trafficking or other forms of harm.</p> <p>Any behaviour that raises concern about grooming must be treated as a safeguarding matter and reported immediately in line with safeguarding procedures, even if no abuse has yet occurred.</p> |
| Exploitation | <p>Exploitation occurs when a child or young person is used, manipulated or coerced by an individual or group for another person’s advantage, gain or gratification, often resulting in harm to the child’s physical, emotional or psychological wellbeing.</p> <p>Exploitation may involve:</p> <ul style="list-style-type: none"> • sexual exploitation, including engaging a child in sexual activity in exchange for affection, attention, money, gifts, status or perceived opportunity • criminal exploitation, including coercion into illegal activity such as theft, drug distribution or other offences • labour or performance exploitation, including forcing or pressuring a child to work, perform or rehearse beyond safe or appropriate limits • financial exploitation, including misuse of a child’s money, earnings or benefits |

| | |
|-----------------------|---|
| | <ul style="list-style-type: none"> • online exploitation, including coercion, blackmail or manipulation via digital platforms. <p>Exploitation often involves an imbalance of power, where the perpetrator uses:</p> <ul style="list-style-type: none"> • age, authority or status • emotional dependency • fear, threats or intimidation • control over access to opportunities or rewards. <p>A child or young person may not recognise exploitation and may appear to be consenting or compliant; however, consent cannot be freely given where exploitation exists.</p> <p>Exploitation can occur alongside grooming, abuse or neglect and may be perpetrated by adults or other children. Any suspicion of exploitation must be treated as a serious safeguarding concern and acted upon immediately in line with safeguarding procedures.</p> |
| Radicalisation | <p>Radicalisation is the process by which a child or young person comes to support, engage in or be influenced by extremist ideologies, beliefs or behaviours, which may lead to the justification of violence, intolerance, hatred or criminal activity.</p> <p>Radicalisation may occur through:</p> <ul style="list-style-type: none"> • exposure to extremist views, propaganda or narratives • manipulation, grooming or coercion by individuals or groups • online platforms, social media, forums or messaging services • peer influence or personal grievance. <p>Children and young people who are being radicalised may be vulnerable due to emotional, social or identity-related factors, and may not initially recognise that they are being exploited or harmed.</p> <p>Radicalisation can occur gradually or rapidly, online or offline, and may involve non-violent extremism that nevertheless creates risk of harm or criminal activity.</p> <p>Concerns relating to radicalisation must be treated as a safeguarding matter and responded to in line with safeguarding procedures, including referral through appropriate statutory channels where necessary, in accordance with the Prevent duty.</p> |

Safeguarding applies online and offline equally.

12. Recognising Indicators

Indicators of abuse or harm

Indicators are signs, signals or patterns of behaviour that may suggest a child or young person is experiencing, or is at risk of, abuse, neglect or exploitation. Indicators do not confirm abuse on their own, but any indicator is sufficient to warrant concern and action.

Indicators may be:

Behavioural indicators

Changes in behaviour or presentation that are out of character or concerning, including:

- withdrawal, isolation or sudden changes in mood
- aggression, anxiety, fearfulness or distress
- regression in behaviour or performance
- reluctance to attend sessions, rehearsals or exams
- excessive compliance, people-pleasing or fear of making mistakes
- inappropriate sexualised behaviour or language.

Physical indicators

Visible signs or physical symptoms that raise concern, including:

- unexplained injuries, bruising or marks
- injuries inconsistent with explanation or developmental stage
- frequent or untreated injuries
- signs of neglect such as poor hygiene, inappropriate clothing or fatigue
- physical pain or discomfort without a clear medical explanation.

Emotional indicators

Indicators relating to a child or young person's emotional wellbeing, including:

- low self-esteem or self-worth
- excessive fear of criticism or failure
- emotional numbness or detachment
- sudden loss of confidence or enjoyment
- heightened sensitivity to feedback or authority figures.

Digital indicators

Indicators arising from a child or young person's online activity or digital behaviour, including:

- secretive or anxious behaviour around devices
- sudden changes in online habits
- receipt of gifts, messages or contacts from unknown individuals
- distress linked to online interactions
- evidence of inappropriate content, grooming or exploitation.

Contextual indicators

Indicators arising from a child or young person's environment, relationships or circumstances, including:

- unsafe supervision or environments
- significant changes in family or care arrangements
- association with concerning peers or adults
- exposure to harmful situations or expectations
- contextual pressures related to performance, competition or opportunity.

Important note

Indicators may appear in isolation or combination, may fluctuate over time, and may be subtle. Staff and examiners are not required to prove abuse - professional concern alone is sufficient to report.

13. Responding to a Disclosure (Mandatory Procedure)

If a child discloses:

1. Listen without interruption
2. Do not ask leading questions
3. Reassure, do not promise confidentiality
4. Record verbatim where possible
5. Report immediately to DSL

If immediate danger: **999**

14. Reporting Pathways & Escalation

Internal

All concerns → DSL immediately

External

DSL refers to:

- Children's Social Care
- Police
- CEOP
- NSPCC

No delay beyond 24 hours.

15. Allegations Against Adults

An allegation against an adult working with or on behalf of I-PATH is any concern that an adult has:

- behaved in a way that has harmed, or may have harmed, a child or young person
- possibly committed a criminal offence against or related to a child
- behaved towards a child or young person in a way that indicates they may pose a risk of harm.



Allegations may relate to staff, examiners, Teacher Members, contractors, volunteers, committee members or any individual acting on behalf of I-PATH, whether the alleged behaviour occurred in person or online, inside or outside an I-PATH activity, or during or outside assessment activity.

1. Child Safety First

The immediate safety and welfare of the child or young person is the paramount consideration at all times. Where a child is believed to be at immediate risk of harm:

- emergency services must be contacted without delay
- appropriate safeguarding measures must be implemented immediately
- the child must be protected from further contact with the alleged individual.

Safeguarding action must not be delayed due to concerns about reputational risk, staffing availability or assessment disruption.

2. Immediate Risk Assessment

Upon receipt of an allegation, the Designated Safeguarding Lead (DSL) will carry out an immediate risk assessment to determine:

- the nature and seriousness of the allegation
- the level of risk posed to the child or other children
- whether the allegation may meet the threshold for statutory intervention
- whether immediate protective measures are required.

The risk assessment will be documented and reviewed as new information emerges.

3. Suspension as a Neutral Act

Where appropriate, the adult may be suspended or temporarily removed from duties as a neutral and protective measure.

Suspension:

- is not a disciplinary sanction
- does not imply guilt or fault
- is used solely to protect children, preserve evidence and maintain the integrity of any investigation.

Alternatives to suspension may be considered only where they fully mitigate risk and are agreed by the DSL.

4. Engagement of Statutory Agencies

Where an allegation meets statutory thresholds, the DSL will:

- make a referral to Children's Social Care, the Police, and/or the Local Authority Designated Officer (LADO) as appropriate
- cooperate fully with statutory investigations
- follow all directions given by external agencies.

I-PATH will not conduct its own investigation where this could interfere with statutory processes.

5. Internal Processes and Case Management

Internal disciplinary, contractual or regulatory processes:

- may run in parallel with external investigations only where appropriate, and
- will be paused or limited where required to avoid compromising external enquiries.

Decisions regarding internal action will be informed by:

- advice from statutory agencies
- legal or regulatory guidance
- safeguarding best practice.

6. Confidentiality and Information Sharing

Information relating to allegations will:

- be shared strictly on a need-to-know basis
- be handled sensitively and confidentially
- be recorded accurately and securely in safeguarding records.

Confidentiality must not be used to prevent the reporting of concerns or to protect individuals from appropriate scrutiny.

7. Outcome and Follow-Up

Following the conclusion of investigations, I-PATH will:

- review outcomes and determine any necessary action
- implement sanctions, restrictions or dismissal where appropriate
- consider referral to the Disclosure and Barring Service (DBS) where required
- provide appropriate support to affected individuals
- review safeguarding practice to identify learning and improvement.

8. Principle of Non-Interference

At all times:

No internal action may compromise or obstruct external safeguarding or criminal investigations. Safeguarding takes precedence over organisational, operational or reputational considerations.

16. Online & Digital Safeguarding

I-PATH recognises that digital delivery and technology-enabled assessment introduce specific safeguarding risks that require heightened controls, clarity of responsibility and robust oversight.

Safeguarding standards apply equally to online, remote and digital environments as they do to face-to-face activity.

This section applies to all activity involving:

- live video examinations (LVE)
- recorded video examinations (RVE)
- online communication, learning and assessment platforms
- digital submission, storage and review of assessment material

1. Core Digital Safeguarding Principles

All online and digital activity must:

- prioritise the safety and welfare of the child or young person
- be transparent, supervised and auditable
- maintain clear professional boundaries
- protect assessment integrity
- comply with safeguarding, data protection and cyber security requirements

Any digital practice that compromises safeguarding or assessment integrity is prohibited.

2. Live Video Examinations (LVE)

For live video examinations:

- only approved platforms authorised by I-PATH may be used
- a responsible adult must be present or available in line with safeguarding requirements
- examiners must never conduct unsupervised 1-to-1 sessions with children
- identity and environment checks must be carried out in line with examination procedures
- examiners must be able to pause or terminate the examination if safeguarding concerns arise
- no private messaging or side-channel communication is permitted during or after the examination

Any unexpected behaviour, environmental concern or technical irregularity must be reported immediately.

3. Recorded Video Examinations (RVE)

For recorded video examinations:

- recordings must be made in a safe, appropriate and supervised environment
- a responsible adult must be aware of and oversee the recording process
- recordings must not place the child or young person at risk of harm, embarrassment or exploitation
- no content may be edited, manipulated or altered in a way that misrepresents the learner or the performance
- recordings must be uploaded via secure, approved submission routes only

Examiners must report concerns where recordings indicate safeguarding risks, coercion, or unsafe practice.

4. Prohibited Practices (Zero Tolerance)

The following are strictly prohibited in all I-PATH online and digital activity:

- private or informal online contact between examiners and learners
- use of unauthorised or personal platforms, accounts or devices
- unsupervised recording of children or young people



- use of artificial intelligence (AI) to manipulate, enhance, alter or generate learner performances
- use of deep-fake technology, synthetic media or digital impersonation
- sharing, storing or distributing recordings outside authorised systems
- screen-recording, copying or repurposing assessment content without permission

Breaches will be treated as serious safeguarding and/or malpractice concerns.

5. Artificial Intelligence and Digital Manipulation

I-PATH explicitly prohibits:

- AI-generated or AI-altered video, audio or imagery in examinations
- digital enhancement of performances (e.g. altering movement, sound, timing or appearance)
- impersonation or substitution using digital tools

Where AI is permitted for learning or preparation, its use must:

- be transparent
- not undermine authenticity
- not be used in assessment submissions
- comply with the I-PATH AI Policy

6. Online Communication and Professional Boundaries

All online communication must:

- be professional, necessary and proportionate
- take place through approved, auditable channels
- avoid private messaging, informal contact or social media engagement

Examiners, staff and Teacher Members must never:

- connect with learners on personal social media
- exchange personal contact details
- continue contact beyond legitimate assessment or safeguarding purposes

7. Digital Environment and Safeguarding Checks

Where applicable, examiners must:

- conduct environment checks (e.g. room scan) in line with examination procedures
- remain alert to safeguarding indicators visible or audible during digital activity
- act immediately where concerns arise

Safeguarding concerns identified online are treated with the same seriousness as those identified in person.

8. Recording, Storage and Data Protection

All digital recordings:

- are treated as sensitive personal data
- must be stored securely



- must only be accessed by authorised individuals
- are retained in line with retention schedules
- are handled in accordance with the Data Protection and Cyber Security Policies

Unauthorised access, sharing or retention constitutes a serious breach.

9. Reporting Digital Safeguarding Concerns

Any concerns relating to online or digital safeguarding must be:

- reported immediately to the Designated Safeguarding Lead (DSL)
- recorded accurately and promptly
- escalated to statutory agencies where thresholds are met

Safeguarding action must not be delayed due to technical, operational or reputational considerations.

10. Enforcement and Sanctions

Failure to comply with digital safeguarding requirements may result in:

- suspension of examination activity
- withdrawal of examiner or centre approval
- investigation under Malpractice, Sanctions or Safeguarding procedures
- referral to external authorities where appropriate

17. Information Sharing & Confidentiality

I-PATH recognises that effective safeguarding depends on the timely, lawful and proportionate sharing of information. Concerns about confidentiality or data protection must never prevent or delay action to protect a child or young person from harm.

1. Safeguarding Overrides Data Protection

Where there is a concern that a child or young person may be at risk of harm:

- safeguarding takes precedence over data protection and confidentiality obligations
- personal data may be shared without consent where this is necessary to protect the child or others
- UK GDPR and the Data Protection Act 2018 explicitly permit information sharing for safeguarding purposes

Failure to share relevant information due to misplaced concerns about data protection is itself a safeguarding risk.

2. Lawful, Proportionate and Purpose-Limited Sharing

All information sharing must be:

- necessary to protect a child or young person
- proportionate to the level of risk identified



- relevant to the safeguarding concern
- accurate and factual, avoiding speculation or opinion
- shared in a timely manner, without unnecessary delay

Only the minimum amount of information required to achieve safeguarding objectives will be shared.

3. Need-to-Know Basis

Safeguarding information is shared strictly on a need-to-know basis, meaning:

- only individuals who require the information to take safeguarding action will receive it
- access is restricted to designated safeguarding roles and relevant authorities
- information is not shared more widely than necessary
- curiosity or interest is not a valid reason for access

All recipients of safeguarding information are expected to maintain confidentiality and handle information responsibly.

4. Consent and Disclosure

Where appropriate and safe:

- consent to share information may be sought

However:

- consent is not required where seeking it would increase risk, cause delay or compromise safeguarding
- a child's refusal to consent does not override the duty to protect them

The rationale for sharing with or without consent must be recorded.

5. Secure Record Keeping

All safeguarding records must be:

- created promptly and factually
- dated, timed and signed
- stored securely in restricted-access systems
- protected from unauthorised access, alteration or loss

Safeguarding records are never stored with general personnel or academic files.

6. Auditability and Accountability

Safeguarding information must be:

- traceable (who recorded, who accessed, who shared, and when)
- retained in line with retention schedules
- available for audit, inspection or regulatory review where required

Records must demonstrate:

- decision-making rationale
- actions taken
- referrals made
- outcomes and follow-up

This ensures transparency, accountability and organisational learning.

7. External Information Sharing

Safeguarding information may be shared with:

- Children's Social Care
- Police
- Local Authority Designated Officers (LADO)
- Health professionals
- the awarding organisation, where relevant to learner protection or assessment integrity

Information is shared securely and in line with statutory guidance.

8. Confidentiality Expectations

All staff, examiners and partners must:

- treat safeguarding information as highly sensitive
- refrain from informal discussion or disclosure
- avoid sharing information via unsecured channels
- comply with I-PATH Data Protection and Safeguarding policies

Breaches of confidentiality may result in disciplinary or regulatory action.

18. Record Keeping

Accurate, secure and well-maintained records are fundamental to effective safeguarding. Safeguarding records provide evidence of concern, decision-making, action taken and outcomes, and must be capable of withstanding external scrutiny.

All safeguarding records must meet the following standards.

1. Factual

Records must be:

- objective and evidence-based
- limited to what was seen, heard, observed or disclosed
- written using clear, plain language
- free from speculation, assumptions or personal opinion

Where interpretation or professional judgement is required, this must be clearly identified as such and supported by observable facts.

Where possible, disclosures should be recorded verbatim, using the child or young person's own words.

2. Timely

Safeguarding records must be:

- made as soon as possible after a concern arises or information is received
- completed on the same day, or within 24 hours at the latest
- updated promptly as new information emerges

Delays in recording can compromise safeguarding action and weaken the reliability of records.

3. Signed

Each record must:

- clearly identify the individual who created it
- include the full name and role of the person making the record
- confirm accountability for the accuracy of the information recorded

Where records are electronic, an identifiable electronic signature or named author is required.

4. Dated

Records must include:

- the date and time the concern was observed or disclosed
- the date and time the record was created
- the date and time of any actions taken, referrals made or decisions reached

Chronology is essential to understanding risk, escalation and response.

5. Securely Stored

Safeguarding records must be:

- stored in secure, access-restricted systems
- protected from unauthorised access, alteration, loss or deletion
- kept separate from general academic, personnel or administrative files

- accessible only to authorised safeguarding personnel

Records must never be stored on personal devices, unsecured drives or informal platforms.

6. Retained Appropriately

Safeguarding records must be:

- retained in line with I-PATH's Data Protection and Retention policies
- kept for as long as necessary to protect the child or others
- available for review, audit or statutory inquiry where required

Records must not be destroyed where there is ongoing risk, investigation or potential future relevance.

Secure disposal must be used once retention periods expire.

7. Accountability and Audit

Safeguarding records must be:

- capable of demonstrating clear decision-making and rationale
- auditable, showing who recorded, accessed and shared information
- sufficient to evidence compliance with safeguarding duties

Good record keeping protects:

- children and young people
- staff and examiners
- the organisation
- the integrity of safeguarding processes

19. Training & Culture

I-PATH recognises that safeguarding is effective only when it is supported by a strong organisational culture, underpinned by high-quality training, clear expectations and active leadership. Safeguarding is not treated as a one-off requirement, but as a continuous, evolving responsibility shared by all.

1. Mandatory Safeguarding Training

I-PATH ensures that all individuals working with or on behalf of the organisation receive safeguarding training that is:

- mandatory prior to undertaking any role involving children or young people
- appropriate to the nature and level of contact with learners
- refreshed regularly to reflect changes in legislation, guidance and risk

Mandatory training covers, as a minimum:

- safeguarding principles and legal duties
- recognising indicators of abuse, neglect and exploitation
- responding to disclosures
- reporting and escalation procedures
- professional boundaries and conduct
- online and digital safeguarding risks

No individual may undertake safeguarding-relevant duties without having completed required training.

2. Role-Specific Guidance and Training

Safeguarding training is tailored to role and responsibility to ensure relevance and effectiveness.

Role-specific guidance is provided for:

- examiners and senior examiners
- staff involved in assessment delivery and quality assurance
- Teacher Members and centres
- committee members and governance roles

This guidance addresses:

- safeguarding risks specific to examinations and assessments
- boundaries in performance and rehearsal contexts
- online and recorded assessment safeguarding
- handling concerns within role-specific authority limits

Generic training alone is not considered sufficient where safeguarding risk varies by role.

3. Designated Safeguarding Lead (DSL) Training

The Designated Safeguarding Lead (DSL) and Deputy DSL receive advanced safeguarding training appropriate to their responsibilities, including:

- managing complex safeguarding cases
- decision-making and threshold assessment
- information sharing and confidentiality
- working with statutory agencies
- handling allegations against adults
- record keeping and audit requirements

DSL training is:

- updated in line with statutory guidance
- refreshed regularly
- supported by professional development and external updates



The DSL has sufficient authority, training and independence to fulfil their role effectively.

4. Safeguarding Embedded into Quality Assurance (QA)

Safeguarding is embedded into I-PATH's quality assurance and governance framework, rather than treated as a separate function.

This includes:

- safeguarding considerations built into policy development
- safeguarding compliance monitored through QA activity
- analysis of safeguarding concerns, trends and near misses
- review of safeguarding practice following incidents
- feedback loops to improve training, guidance and procedures

Safeguarding performance informs:

- examiner approval and continuation
- centre approval and monitoring
- risk assessment and procedural updates

5. Culture of Vigilance and Professional Curiosity

I-PATH actively promotes a safeguarding culture where:

- concerns are raised early and without fear
- staff and examiners are encouraged to exercise professional curiosity
- safeguarding is prioritised over operational convenience
- silence, minimisation or inaction are not tolerated

Individuals are supported to challenge unsafe practice and escalate concerns appropriately.

6. Accountability and Continuous Improvement

Safeguarding training and culture are monitored through:

- training records and compliance tracking
- policy review and update cycles
- internal audit and governance reporting
- awarding organisation oversight

Learning from safeguarding cases is used to strengthen systems, guidance and training.

20. Whistleblowing

I-PATH is committed to creating an environment in which individuals feel safe, supported and confident to raise concerns about safeguarding, misconduct or unsafe practice. Whistleblowing is recognised as a critical safeguarding safeguard and an essential component of organisational integrity.

1. Right and Duty to Raise Concerns

All staff, examiners, Teacher Members, contractors, volunteers and partners have both:

- the right, and
- the professional responsibility

to raise concerns where they believe:

- a child or young person is at risk of harm
- safeguarding procedures are not being followed
- unsafe, unethical or inappropriate behaviour is occurring
- safeguarding concerns are being ignored, minimised or suppressed.

Concerns may relate to actions, omissions, practices or decisions.

2. No Fear of Reprisal

Concerns may be raised:

- without fear of victimisation, retaliation or disadvantage
- regardless of seniority, role or relationship

I-PATH will not tolerate:

- intimidation
- discrimination
- harassment
- penalisation

against any individual who raises a concern in good faith.

Any attempt to discourage, silence or penalise whistleblowers will itself be treated as a serious safeguarding and disciplinary matter.

3. How to Raise a Concern

Concerns should normally be raised:

- with the Designated Safeguarding Lead (DSL)

Where this is not appropriate, concerns may be raised:

- directly with Head Office
- with a member of the Grand Council
- through external whistleblowing routes where necessary.



Concerns may be raised verbally or in writing and should be supported by factual information where possible.

4. Confidentiality and Anonymity

- Whistleblowers' identities will be protected wherever possible
- Information will be shared only on a need-to-know basis
- Anonymous concerns will be considered where credible information is provided

Confidentiality will not prevent appropriate investigation or referral to statutory agencies where required.

5. Response and Investigation

All whistleblowing concerns will be:

- taken seriously
- assessed promptly
- handled sensitively and proportionately
- escalated where safeguarding thresholds are met

Whistleblowing concerns relating to safeguarding will be managed under safeguarding procedures and may involve statutory agencies.

6. Failure to Whistleblow

Failure to raise a safeguarding concern, including:

- ignoring indicators of abuse
- failing to report unsafe practice
- remaining silent due to fear, loyalty or convenience

constitutes a serious safeguarding failure.

Where appropriate, failure to whistleblow may result in:

- investigation
- disciplinary action
- withdrawal of approval or role
- regulatory or external referral.

7. External Whistleblowing Routes

Where internal routes are not appropriate or have been exhausted, individuals may raise concerns with:

- the NSPCC Whistleblowing Advice Line (0800 028 0285)
- local authority safeguarding teams
- the Police

I-PATH supports individuals who choose to escalate concerns appropriately.

21. Complaints vs Safeguarding

I-PATH recognises that not all concerns raised through formal or informal channels are complaints. Where a concern involves, or may involve, the safety, welfare or protection of a child or young person, it must be treated as a safeguarding matter, not a customer service issue.

Safeguarding concerns must never be downgraded, reframed or managed solely as complaints.

1. Safeguarding Takes Precedence

Where a concern:

- suggests a child or young person may be at risk of harm
- involves inappropriate conduct, boundaries or behaviour
- raises questions about abuse, neglect or exploitation
- involves allegations against an adult or peer

it must be escalated immediately through safeguarding procedures, regardless of:

- how the concern is raised
- who raises it
- the perceived seriousness
- reputational or operational impact.

Complaints procedures must not delay or replace safeguarding action.

2. Complaints That Trigger Safeguarding

A complaint may become a safeguarding matter where it includes:

- allegations of harm or risk of harm
- concerns about professional boundaries
- unsafe supervision or practice
- emotional distress, fear or intimidation
- inappropriate digital contact or behaviour

In such cases:

- safeguarding procedures take precedence
- the Designated Safeguarding Lead (DSL) must be notified immediately
- safeguarding thresholds and statutory referral considerations apply.

3. Parallel Processes (Where Appropriate)

Where a matter contains both:

- safeguarding elements, and

- service or procedural issues

the processes may run in parallel, but:

- safeguarding action always comes first
- complaints handling must not interfere with safeguarding investigation
- outcomes of safeguarding processes may inform complaint resolution, not the reverse.

4. No Informal Resolution of Safeguarding

Safeguarding concerns must never be:

- informally “resolved”
- managed through mediation
- handled solely through customer service responses
- minimised to avoid escalation

Any attempt to manage safeguarding concerns informally constitutes a safeguarding failure.

5. Record Keeping and Audit Trail

Where a complaint is identified as, or escalated to, a safeguarding concern:

- the rationale for escalation must be recorded
- safeguarding records must be created and maintained
- actions and decisions must be auditable

This ensures transparency, accountability and regulatory compliance.

6. Staff Responsibilities

All staff, examiners and partners must:

- remain alert to safeguarding indicators within complaints
- escalate concerns immediately
- avoid making threshold judgments beyond their role
- understand that misclassification of safeguarding concerns is itself a risk.

22. Monitoring, Audit & Continuous Improvement

I-PATH recognises that safeguarding is not static and must be actively monitored, scrutinised and continuously improved. Robust oversight ensures that safeguarding arrangements remain effective, proportionate and responsive to emerging risks.

1. Incident Review

All safeguarding incidents, concerns and near misses are subject to systematic review.

Incident review includes:

- analysis of the nature and seriousness of concerns
- evaluation of response times and decision-making
- assessment of actions taken and outcomes achieved
- identification of any procedural or training gaps

Where appropriate, post-incident reviews are conducted to:

- identify learning
- strengthen safeguards
- prevent recurrence

Serious incidents are escalated to governance without delay.

2. Trend Analysis

I-PATH undertakes regular analysis of safeguarding data to identify patterns, trends or emerging risks.

Trend analysis may consider:

- frequency and type of safeguarding concerns
- online vs face-to-face safeguarding issues
- centre-, discipline- or role-specific patterns
- recurring themes or systemic weaknesses

Findings inform:

- policy review
- training priorities
- risk assessments
- quality assurance focus

3. Governance Reporting

Safeguarding is reported through formal governance structures.

This includes:

- regular safeguarding updates to the Grand Council
- reporting on serious incidents, emerging risks and trends
- assurance on compliance with safeguarding policies
- review of training completion and effectiveness

Governance bodies are expected to:

- challenge safeguarding performance
- ensure accountability
- authorise improvements and resource allocation

Safeguarding is treated as a standing governance agenda item, not an exception report.

4. Awarding Organisation Oversight

Where safeguarding relates to regulated qualifications, I-PATH:

- engages transparently with the awarding organisation
- shares relevant safeguarding information where appropriate
- responds to safeguarding feedback or recommendations
- incorporates awarding-organisation guidance into practice

The awarding organisation's oversight supports:

- alignment with regulatory expectations
- sector benchmarking
- continuous improvement of safeguarding standards

5. Continuous Improvement Cycle

Safeguarding improvement follows a continuous improvement cycle:

1. Identify risks and incidents
2. Analyse data and trends
3. Review policies and procedures
4. Implement improvements
5. Monitor impact

This cycle ensures safeguarding remains effective and responsive.

6. Accountability and Evidence

All monitoring and audit activity is:

- documented
- auditable
- capable of evidencing decision-making and improvement

This ensures I-PATH can demonstrate safeguarding effectiveness to:

- regulators
- awarding organisations
- statutory agencies

23. Key Contacts

DSL: Dr Adam Tate

Email: info@i-path.org

NSPCC: 0808 800 5000

CEOP: www.ceop.police.uk

Emergency: 999