

Element Society safeguarding children policy

Staff-facing policy for education, alternative provision, holiday delivery, youth work and community activity

Policy number	SAFE-001
Status	Approved
Version	July 2026
Owner	Christopher Hill, Designated Safeguarding Lead
Deputy DSL	Cleo Metcalf
Safeguarding Trustee	Ian Balshaw
Approval body	Chair of Trustees, on behalf of the Board of Trustees
Applies to	All Element Society work with children and young people under 18, including education, AP, HAF, youth work, outreach, online contact, one-to-one work, home visits, transport, trips and community activity.
Review	Next review by August 2027, and sooner after legal, funder, service, serious incident or material risk change.
Supersedes	Element Society Safeguarding Children Policy live staff-facing version June 2026 and the July 2026 filtering/monitoring amendment document.

Use this staff-facing version for day-to-day practice. It keeps the quick action sheet at the front, retains the operational strength of the June 2026 live policy, and incorporates the July 2026 filtering and monitoring updates from the self-audit work.

Use Appendix 1 and the internal contact list for live contact details and local routes. Use the AP quick pull-out and AP operational annex wherever AP delivery is involved.

Safeguarding quick action sheet

Recognise	Take seriously any disclosure, injury, behaviour change, peer-on-peer abuse, exploitation indicator, online concern, repeated absence, a child leaving session or site, or anything that does not feel right.
Respond	Listen. Stay calm. Reassure the child they have done the right thing. Do not promise confidentiality. Do not investigate or ask leading questions. Make the situation as safe as possible.
Record	Write a factual account on the same day. Use the child's own words where possible. Include date, time, place, who was present, what you saw or heard, and what you did next.
Report	Pass the concern to the DSL or Deputy DSL straight away. In AP, follow the same-day calls and council incident form route set out in the AP quick pull-out.
Refer	The DSL or Deputy DSL will usually lead referrals, but any member of staff can make a direct referral if there is immediate risk, the DSL is unavailable, or they believe action is not being taken quickly enough.
Escalate	Immediate danger: call 999. Concern about Christopher Hill: go to Ian Balshaw. Concern about Ian Balshaw: go to trustees@elementsociety.co.uk and/or Sheffield Safeguarding Hub. Concern about poor or unsafe practice: use the low-level concerns or whistleblowing route and record the escalation.

Do - Share concerns early. - Use need-to-know information sharing. - Keep the child at the centre. - Follow up if you do not receive a response.	Do not - promise to keep a secret. - question the child repeatedly. - delay because you are unsure. - assume someone else has dealt with it.
--	--

1. Purpose and principles

Element Society is committed to safeguarding and promoting the welfare of every child it works with. Safeguarding is everybody's responsibility. Element takes a child-centred approach and acts on concerns early.

For the purpose of this policy, a child is anyone under 18. Adults at risk are covered under Element Society's separate safeguarding adults policy.

Element works with the whole child in their family, peer, school and community context, but the child's welfare remains paramount. Staff should think about immediate safety, longer-term risk, and who else needs to know or act.

2. Scope

This policy applies to trustees, staff, sessional workers, agency staff, volunteers, students, contractors and anyone acting on behalf of Element Society where children are present or may be affected by our work.

It applies across Element's child-facing work, including educational work and alternative provision, Holiday Activities and Food delivery, detached and outreach youth work, open-access youth work and youth club delivery, one-to-one work, home visits, transport, trips, and online or phone-based contact.

Element does not currently run residential programmes. If residential work resumes, a separate residential safeguarding addendum must be approved before delivery starts.

3. Legal and guidance framework

This policy is written against the current safeguarding framework in England at the date of issue. It has regard to the Children Act 1989 and 2004, the current version of Working Together to Safeguard Children, and Charity Commission safeguarding guidance for trustees.

Where Element delivers education or alternative provision, it also has regard to the current version of Keeping Children Safe in Education, the current information-sharing advice for safeguarding practitioners, the current statutory guidance on alternative provision, the current Children Missing Education statutory guidance, and current DfE digital and technology standards for filtering and monitoring.

The July 2026 edition also reflects the July 2026 self-audit updates on online safety, acceptable use, staff monitoring/privacy, IT systems records, and filtering and monitoring assurance. Where official guidance changes, the current official version takes priority and this policy must be reviewed.

Local Sheffield procedures, including the Sheffield Safeguarding Hub, Sheffield LADO route and Sheffield alternative provision processes, must be followed for Sheffield children unless the child lives elsewhere and another local authority route must be used.

4. Leadership, oversight and linked documents

Element uses the role titles DSL, Deputy DSL and Safeguarding Trustee. This language fits current national education guidance and is clearer for mixed delivery across education, AP, HAF and youth work.

Where this policy refers to the DSL, the Deputy DSL may act with the same authority when covering or when delegated.

Role	Responsibilities
Board of Trustees	Retains overall safeguarding responsibility, sets culture and oversight, assures resources and training, receives safeguarding assurance, and reviews policy and learning at least annually. The Board must receive enough assurance to know that safeguarding and online safety controls are being used in practice.
Safeguarding Trustee	Acts as the board safeguarding lead and escalation point for concerns about the CEO/DSL. Provides oversight and challenge rather than routine case handling, unless the escalation route requires it.
Designated Safeguarding Lead	Leads safeguarding practice, advises staff, makes or oversees referrals, liaises with statutory agencies, schools and commissioners, manages secure records and chronologies, leads the safeguarding response to online concerns and oversees policy review.
Deputy DSL	Trained to the same standard as the DSL and provides operational cover. May advise staff, receive reports, make referrals, escalate, review concerns and manage cases when covering or when delegated.
Managers and project leads	Ensure staff know this policy, staffing and risk controls are in place, attendance and incident systems are followed, online and site risks are managed, and concerns are escalated immediately.
Operational digital or IT lead / contracted IT support	Maintains filtering and monitoring systems where Element manages devices, networks, accounts or digital systems used for education, AP or youth work; completes technical checks; provides reports; records actions; and works with the DSL and senior leaders to make prompt changes where gaps or new risks are identified.

Role	Responsibilities
All staff, volunteers and trustees	Read and follow this policy, recognise concerns, record and report promptly, challenge unsafe practice, follow acceptable use rules, report system weaknesses, and take direct action when delay would place a child at risk.

Linked controlled documents

Document	Purpose
AP safeguarding quick pull-out and AP operational annex	Apply to all AP delivery and set out the same-day route, attendance rules and placement-level operational requirements.
Online Safety and E-Safety Policy IT-007 July 2026	Sets operational rules for online safety, filtering, monitoring, reporting routes, online harms and education expectations.
FM-001 Filtering and Monitoring Review Checklist July 2026	Termly safeguarding and technical evidence record for AP/education and annual organisation-wide review.
HR-025 Staff Acceptable Use Agreement July 2026	Sets the rules for Element-owned devices, accounts, networks, personal device restrictions, staff online conduct and awareness of filtering, logging and proportionate monitoring.
HR-PRIV-001 Staff Privacy Notice July 2026	Explains what may be filtered, logged or monitored on Element-owned devices and networks, why this is done, who can access records, retention and staff rights.
IT-001 Data Protection Policy July 2026	Covers UK GDPR, lawful sharing, children's data, records, breaches, SARs and governance.
IT-002 Information Security, Retention and Disposal Policy July 2026	Covers secure storage, access controls, retention, disposal and records management.
IT-006 IT Systems Register July 2026	Records approved systems, owners, data categories, controls and review status.
DPIA-FM-001 Filtering, Monitoring and Device Controls	Must be completed or recovered as the DPIA evidence for filtering, monitoring and device controls. Until complete, this remains an implementation action.
Staff Code of Conduct and safer working practice	Sets professional boundaries, communication rules, touch, lone working expectations, gifts, social media and standards of behaviour.
Low-level concerns and Whistleblowing	Explains how to raise concerns about adult conduct, unsafe practice, poor culture or failed safeguarding responses.
Safer Recruitment and DBS	Covers role design, vetting, references, induction, supervision and what happens when checks are delayed or a role changes.
Lone Working, Home Visits and Community Delivery	Covers detached work, outreach, visits, communication plans, dynamic risk assessment and staff escalation routes.
Transporting Children	Covers driver authorisation, vehicle checks, supervision, consent, collection and emergency procedures.
Health and Safety, First Aid and Incident Reporting	Covers accidents, site safety, medical needs, emergency response and how health and safety reporting links to safeguarding.
Complaints	Provides a route for children, families, schools, partners or staff to raise service concerns that are not dealt with through safeguarding procedures alone.
Safeguarding adults policy	Applies to adults at risk and must be used whenever work includes 18+ participants or a mixed-age context creates an adult safeguarding issue.

5. Recognising concerns

Abuse, neglect and exploitation can happen in families, peer groups, institutions, online spaces and community settings. Staff must be professionally curious and should be alert to immediate incidents, patterns over time and changes in presentation or attendance.

- physical abuse, emotional abuse, sexual abuse and neglect
- child-on-child abuse, including sexual violence, sexual harassment, harmful sexual behaviour, bullying and coercive control
- child sexual exploitation, child criminal exploitation, county lines, trafficking and modern slavery
- domestic abuse, so-called honour-based abuse, forced marriage and female genital mutilation
- online abuse, grooming, harmful content, image-sharing abuse, deepfakes, AI misuse, extremism, radicalisation, fraud and coercion
- extra-familial harm, including harm in public places, peer groups and community settings
- repeated or unexplained absence, missing episodes, children leaving sessions without permission, and wider welfare concerns linked to attendance

Staff do not need proof before acting. A concern may arise from what a child says, what staff see, what another person reports, a pattern across time, or a strong professional sense that something is wrong.

6. What all staff and volunteers must do

When a child discloses, or when you witness or suspect abuse:

- make the situation as safe as possible
- listen carefully and stay calm
- take the child seriously
- do not promise confidentiality
- do not ask leading questions or investigate
- tell the DSL or Deputy DSL immediately and on the same day
- write a factual record the same working day
- follow up and escalate if you do not receive a response that matches the level of risk

The DSL or Deputy DSL will usually decide the next step and make referrals. However, any member of staff may make a direct referral to Children's Social Care or the police if a child is at immediate risk, if the DSL or Deputy DSL cannot be reached, or if the response appears too slow for the level of concern.

Responding to immediate danger or urgent medical need:

- call 999 without delay
- follow emergency services advice
- tell the DSL or Deputy DSL as soon as it is safe to do so
- preserve evidence where possible and do not interfere with potential evidence

7. Recording concerns

Safeguarding records must be clear, factual, timed, dated and signed. Staff must record the child's own words where possible and separate fact, observation, opinion and action.

A good record will include:

- the date, time and place of the concern or disclosure
- what was seen, heard or said
- the exact words used by the child, where possible
- what action was taken and by whom
- who the concern was shared with and when
- any decision made not to refer externally, and the rationale for that decision

Records must be stored securely and shared only on a need-to-know basis for safeguarding purposes. Safeguarding information must not be kept in informal notebooks, personal devices, unsecured message threads, WhatsApp, social media messages or email inboxes as the only record.

Where filtering, monitoring, online safety or device-use information identifies a safeguarding concern, the safeguarding concern must be recorded in the safeguarding record system or approved safeguarding route. Technical logs may support the record but do not replace safeguarding recording.

8. Information sharing and confidentiality

Element shares information lawfully and proportionately to safeguard children. Consent should usually be sought for early help and supportive information sharing, but consent is not needed where there is a safeguarding or child protection reason to share. Data protection is not a barrier to keeping children safe.

Children and families should normally be told what information is being shared and why, unless doing so would place a child or another person at increased risk, prejudice a police or social care process, or create another good safeguarding reason not to do so.

When a child moves school, setting or service, relevant safeguarding information should be transferred securely and without unnecessary delay.

9. Early help

Not all safeguarding concerns require statutory child protection action. Element may identify children and families who would benefit from early help. Staff should discuss this with the DSL or Deputy DSL and decide whether an early help conversation, assessment or referral is needed.

Early help is usually collaborative and voluntary. Where seeking consent would place a child at greater risk, staff must seek DSL advice and consider a safeguarding referral instead.

10. Referrals to Children's Social Care, police and other agencies

The DSL or Deputy DSL will normally lead referrals and multi-agency liaison. This includes referrals to Children's Social Care, the police, health services, Prevent or Channel processes, CEOP where relevant, and local authority services.

For children who live in Sheffield, referrals should follow current Sheffield procedures. For children from another area, Element must use the relevant local authority and school routes for that child, but must not delay emergency action while working out who owns the case.

Where a referral is not accepted or the response does not appear to match the level of concern, the DSL or Deputy DSL should escalate through professional challenge and record what was challenged, to whom, when and with what outcome.

11. Service-specific safeguarding arrangements

Alternative provision and educational work

Alternative provision and education work must operate to this policy and the current AP safeguarding documents. The AP quick pull-out covers the same-day operational steps. The AP operational annex covers the wider pre-start, attendance, information-sharing and review expectations for placements.

Where a child is on a school roll, the commissioning school remains a key safeguarding and attendance partner. Where a child is not on roll and the local authority or another service is the education lead, Element must know the named education lead and the named safeguarding contact before delivery starts.

Holiday and activity programmes

Before children attend, staff must have the registration, emergency contact, collection, medical and relevant risk information needed for safe delivery. Staff must know who has parental responsibility where this affects collection, consent or information sharing.

Detached, outreach and open-access youth work

Detached and outreach work must follow the approved risk assessment, communication plan and lone working controls. Staff must not take children to unplanned private locations, must use approved communication routes, and must manage welfare concerns in a child-centred but professionally boundaried way.

One-to-one work, home visits and transport

One-to-one work, home visits and transport must be authorised, risk assessed and carried out under the relevant Element procedure. Staff must use approved routes, keep records and escalate any safeguarding or welfare concern that arises during the activity.

Online and phone-based contact

Only approved devices, accounts and platforms must be used for work with children. Staff must not use personal social media or informal private messaging with children. Any exceptional emergency contact arrangement must be agreed and recorded.

12. Children absent from education, repeated absence, missing episodes, uncollected children and leaving without permission

Unexpected absence, non-arrival, repeated unexplained absence, prolonged absence, not being collected, going missing, or leaving without permission may all have safeguarding implications. In education and AP contexts these issues must also be considered through the lens of attendance and children missing education.

When any of these issues arise, staff must:

- record what has happened and what checks have been made
- inform the DSL or Deputy DSL promptly and on the same day where risk or pattern is present
- inform parent, carer, school or commissioner where required by the activity or placement arrangement
- contact the police where the level of risk requires it
- treat repeated or prolonged unexplained absence in education or AP as a safeguarding concern, not just an attendance problem
- review patterns over time and escalate where exploitation, neglect, family breakdown, mental health crisis or other risk may be present

AP-specific attendance, first-day absence and leaving-site rules are set out in the AP safeguarding documents and must be followed exactly.

13. Online safety, filtering and monitoring

Online safety is a running and interrelated safeguarding theme across Element's work. Children may be harmed online and offline, and the two often overlap. Online harms can include bullying, coercion, sexual abuse, exploitation, exposure to extremist material, harmful challenges, self-harm content, image-sharing abuse, fraud, deepfakes, the misuse of generative AI and other digital tools.

Element maintains appropriate filtering and monitoring arrangements for internet access and Element-owned devices, networks, accounts and digital systems used in education, AP and youth work delivery. These arrangements are set out in the Online Safety and E-Safety Policy, Staff Acceptable Use Agreement, Staff Privacy Notice, IT Systems Register, Filtering and Monitoring Review Checklist and the related DPIA.

Technical controls support safeguarding, but they do not replace professional vigilance, active supervision, safe relationships, staff curiosity, clear behaviour expectations and same-day safeguarding reporting.

Role	Filtering and monitoring responsibility
Board / senior leadership	Ensure appropriate filtering and monitoring systems are in place for Element-owned devices, networks, accounts and digital systems used in education, AP, youth work or direct delivery with children and young people. Review effectiveness at least annually, and sooner when risk, technology or delivery changes.
DSL / Deputy DSL	Lead the safeguarding response to online concerns, review relevant alerts or reports, identify patterns, decide follow-up action, and provide assurance upward that online risks are being managed.
Operational digital or IT lead / contracted IT support	Maintain the systems, run checks, provide reports, record technical actions, and work with senior leaders and the DSL to make prompt changes where gaps or new risks are identified.
Managers and project leads	Check that the right devices, accounts and networks are being used in delivery, that staff understand the rules, and that any weaknesses are reported promptly.
All staff	Supervise use, follow acceptable use and image-sharing rules, report concerns and system weaknesses, and never rely solely on technical controls to keep children safe.

Filtering and monitoring arrangements must reflect how Element actually works, including devices taken off site, third-party venues, bring-your-own-device risks, live online contact, social media, work mobile messaging and any use of new technology. Where delivery takes place on a third-party network or premises, the risks and available safeguards must be checked before the activity starts.

Staff must report online safety concerns and system weaknesses immediately. Examples include harmful or inappropriate search results, blocked access being bypassed, missing filtering on a device, unexpected alerts, unsafe group chats, nude or semi-nude image-sharing, cyberbullying, grooming indicators, self-harm content, extremist content, AI misuse or any online issue that affects safety offline.

The DSL or Deputy DSL decides whether an online safety issue is a safeguarding concern, a behaviour issue, an IT/security issue, a data protection issue, or a combination. Safeguarding action must not be delayed while technical checks are being completed.

Staff must not view, copy, save, forward, print or share sexual images of a child unless the DSL has agreed there is a clear safeguarding reason and the action is necessary and proportionate. Staff must seek DSL advice and follow the online safety policy and relevant guidance.

Filtering and monitoring evidence must be retained through the approved evidence route. This includes completed FM-001 reviews, technical reports, action logs, system changes, incidents, near misses and learning. Safeguarding records must contain enough information to explain the concern and action taken without storing unnecessary technical data or images.

14. Child-on-child abuse

Element recognises that children can abuse other children and that this can happen in any service. This includes bullying, prejudice-based behaviour, sexual violence, sexual harassment, upskirting, harmful sexual behaviour, coercive control, initiation or hazing-type behaviour, and online abuse between children.

All reports must be taken seriously. Element will not dismiss harmful behaviour as banter, growing up, or part of youth culture. Victims will be supported, alleged perpetrators managed proportionately, and the wider context considered.

15. Prevent, radicalisation and contextual harm

Safeguarding includes protecting children from radicalisation, extremism and other forms of extra-familial harm. Staff should be alert to changes in behaviour, online activity, language, associations, unexplained money, unexplained injuries, fear, missing episodes or patterns that suggest coercion or exploitation.

Concerns about radicalisation must be reported to the DSL or Deputy DSL. Prevent or Channel referrals should be made where appropriate, in line with local procedures.

16. Safer working practice

All adults working with children through Element must maintain professional boundaries and follow the Staff Code of Conduct. This includes appropriate language, safe touch, gifts, transport, online contact, the use of images and avoiding private or exclusive relationships with children.

- staff must not promise secrecy or create exclusive relationships with children
- staff must not use personal devices or personal social media to communicate with children unless a separate authorised emergency arrangement has been agreed and recorded
- physical contact must be appropriate, necessary, proportionate and in line with training, risk assessment and the child's needs
- any boundary slip, no matter how small, must be discussed with a manager, the DSL or Deputy DSL

17. Low-level concerns, unsafe practice, whistleblowing and allegations about adults

Element will respond promptly and fairly to concerns about staff, volunteers, trustees, contractors and anyone working with children on its behalf. This section applies both to lower-level concerns and to allegations that may meet the harm threshold.

Low-level concerns about adults

A low-level concern is any concern, no matter how small, that an adult working with children may have acted in a way that is inconsistent with the Staff Code of Conduct, creates discomfort or uncertainty, or could develop into a pattern of poor practice, but does not clearly meet the harm threshold.

- Report low-level concerns about any adult other than Christopher Hill to Christopher Hill or Cleo Metcalf.
- Report low-level concerns about Christopher Hill to Ian Balshaw.
- Report low-level concerns about Ian Balshaw to trustees@elementsociety.co.uk.
- Adults are expected to self-report if they find themselves in a situation that could be misinterpreted or that falls below expected professional standards.

All low-level concerns must be recorded in writing, including the context, any action taken and any pattern review. Records must be kept securely and reviewed so that repeated, problematic or escalating behaviour can be identified and acted on.

Unsafe practice and whistleblowing

Unsafe safeguarding practice includes poor decision-making, failure to report, pressure not to report, tampering with records, unsafe staffing or supervision, repeated boundary issues, or a culture in which concerns are minimised. Concerns about unsafe practice should be raised with a manager, the DSL, the Deputy DSL or the Safeguarding Trustee as appropriate.

If a member of staff feels unable to raise a concern internally, or believes the internal response is unsafe or inadequate, they should use Element's Whistleblowing Policy and may also use an external route such as the NSPCC whistleblowing helpline or the relevant local safeguarding route. No one should suffer detriment for raising a genuine concern in good faith.

Concerns or allegations that may meet the harm threshold

Where the concern suggests that an adult who works with children may have harmed a child, may have committed a criminal offence related to a child, may pose a risk of harm to children, or may not be suitable to work with children, the case manager must seek LADO advice or make a LADO referral within one working day and follow local procedures. Staff must not investigate these cases themselves before advice is taken, other than taking immediate steps to protect a child or preserve evidence.

Concern route	Action
Concern about a staff member, volunteer, sessional worker, contractor, agency worker or student placement	Report immediately to Christopher Hill or Cleo Metcalf. Christopher Hill acts as case manager unless unavailable or implicated. Where the adult is employed by another organisation, that employer must also be informed.
Concern about Christopher Hill	Report immediately to Ian Balshaw. Ian Balshaw acts as case manager for this route and must seek LADO advice or referral where threshold may be met.
Concern about Ian Balshaw	Report to trustees@elementsociety.co.uk and/or Sheffield Safeguarding Hub. The Board of Trustees must appoint an unconflicted trustee case manager. If urgent action is needed, do not wait for a board process before contacting the local safeguarding route.
Concern about an adult from another organisation on a shared site or partnership activity	Tell the Element DSL or Deputy DSL and that organisation's senior manager. The employing organisation will normally be the case manager, but Element must still take immediate protective action and escalate if the response is unsafe or too slow.

At the end of a substantiated case, or when a person is removed from regulated activity or would have been removed had they not left, Element will consider DBS and any other regulator or commissioning notifications required by law or contract.

18. Safer recruitment, induction and training

Element uses safer recruitment measures appropriate to role and legal eligibility, including DBS checks where roles qualify, references, identity checks, role clarity, induction and supervision.

No adult should begin unsupervised work with children until the required recruitment and induction steps are complete.

All staff and volunteers must receive safeguarding induction, know the reporting route, understand the Code of Conduct, acceptable use rules and online safety expectations, and receive regular safeguarding updates. Training and briefings should reflect the reality of Element's work, including AP, youth work, detached practice, online safety, filtering and monitoring, low-level concerns, child-on-child abuse and contextual safeguarding.

19. Working with parents, carers, schools and other partners

Element aims to work openly and constructively with parents, carers, schools, commissioners and partner agencies wherever this is safe and appropriate. Good safeguarding depends on timely, respectful and accurate information sharing.

In AP and other commissioned work, Element must be clear about who the commissioning school or education lead is, who the named safeguarding contact is, and who is responsible for attendance, welfare and emergency decisions on the day.

20. Governance, review and learning

This policy must be reviewed at least annually and after any serious safeguarding incident, serious near miss, major service change, significant technology change or significant change in law or guidance. The review should take account of staff learning, safeguarding themes, allegations, complaints, audits, online safety evidence, filtering and monitoring reviews, commissioner feedback and lessons learned from practice.

The Board of Trustees retains overall safeguarding responsibility even where day-to-day safeguarding functions are delegated. Trustees should receive enough information and challenge to assure themselves that safeguarding arrangements are being used in practice, not simply written down.

The July 2026 launch must be supported by a policy issue record, staff briefing or communication, staff acknowledgement route, updated linked policy library, completed filtering and monitoring review, and a confirmed position on DPIA-FM-001.

Appendix 1. Quick reference contacts

Update this appendix whenever contact details change. Keep numbers and local routes here rather than throughout the policy. If sharing externally beyond trusted commissioners or auditors, consider a redacted contact appendix.

Contact type	Name / route	Contact	Use / note
Element DSL	Christopher Hill	chris.h@elementsociety.co.uk / 07510 045499 / 07701 064533	Check against the live internal contact list if details change.

Contact type	Name / route	Contact	Use / note
Element Deputy DSL	Cleo Metcalf	Use the live internal staff contact list / agreed on-day cover route.	Do not leave a session running without a known Deputy DSL contact route.
Safeguarding Trustee	Ian Balshaw	ian.b@elementsociety.co.uk / 07581 071231	Escalation route for concerns about Christopher Hill.
Trustee escalation	Trustees	trustees@elementsociety.co.uk	Use for concerns about Ian Balshaw or where an unconflicted trustee case manager is needed.
Emergency / police	Emergency and non-emergency	999 / 101	999 for immediate danger. 101 for non-emergency police matters.
Sheffield Safeguarding Hub	Children's Social Care	0114 273 4855	Use the current Sheffield child safeguarding route for Sheffield children.
Sheffield LADO	New referrals and advice	New referrals via Sheffield Safeguarding Hub option 3 / sheffieldsafeguardinghub@sheffield.gov.uk / follow-up: LADO@sheffield.gov.uk	For concerns about adults who work with children.
Whistleblowing	NSPCC	0800 028 0285	External route if a staff member feels unable to raise safeguarding practice concerns internally.

Appendix 2. Filtering and monitoring assurance summary

This appendix summarises the safeguarding control position. The operational evidence must sit in FM-001, IT-006, HR-025, HR-PRIV-001, IT-001, IT-002 and DPIA-FM-001.

Area	Required assurance
Ownership	DSL/Online Safety Lead owns safeguarding response. Operational digital or IT support maintains technical controls. Board receives assurance.
Review frequency	Termly for AP/education and whenever systems, risks or delivery arrangements change. At least annually organisation-wide.
Coverage	Element-owned devices, approved work accounts, managed networks and relevant digital systems used in education, AP, youth work and direct delivery with children. Third-party venues must be checked through delivery risk assessment.
Filtering	Filtering should block harmful and inappropriate content without unreasonably restricting legitimate learning, support or youth work activity. Weaknesses must be reported and logged.
Monitoring	Monitoring arrangements must meet safeguarding need, identify relevant concerns, and have a clear route for review, triage, action and record keeping.
Alerts and reports	Alerts or reports with safeguarding relevance are reviewed by the DSL/Deputy DSL or delegated safeguarding lead. Decisions and actions are recorded.
Staff awareness	Staff receive the acceptable use agreement and privacy notice. Staff know what may be filtered, logged or monitored and how to report concerns.
Data protection	Monitoring must be necessary, proportionate, transparent where safe, securely retained, access restricted and covered by privacy information and DPIA.
Evidence location	FM-001 completed reviews, IT Systems Register, DPIA-FM-001, incident/near miss logs, safeguarding records, technical action logs and board/SLT assurance notes.
Open action	DPIA-FM-001 approved 26 August 2026. Lightspeed post-install review due by 31 August 2026 before live use from 1 September 2026.

Appendix 3. July 2026 launch checklist

Action	Owner	Evidence
Chair of Trustees approval recorded.	CEO / Chair	Signed approval record / DocuSign.
June 2026 policy and July 2026 safeguarding amendment document marked superseded.	CEO / Policy owner	Policy register updated.

Action	Owner	Evidence
July 2026 linked documents issued: IT-007, HR-025, HR-PRIV-001, IT-001, IT-002, IT-006 and FM-001.	CEO / DSL / SLT	Policy issue email or staff briefing record.
Staff acknowledgment collected for safeguarding policy and acceptable use agreement.	Managers	BreatheHR policy read records / acknowledgement log.
Filtering and monitoring review completed using FM-001.	DSL / IT support / SLT	Completed FM-001 record.
DPIA-FM-001 approved and post-install review scheduled.	DSL / Data lead	Approved DPIA record.
AP quick pull-out and AP operational annex checked for consistency with this policy.	DSL / AP lead	Version check note.
Internal contact list checked against Appendix 1.	DSL / Office lead	Updated internal contact list.

Appendix 4. Document history and sign-off

Version	Date	Summary
June 2026	03 June 2026	Live staff-facing safeguarding children policy signed/approved for internal use.
July 2026 amendment	July 2026	Filtering and monitoring wording rebuilt following self-audit.
July 2026 merged launch edition	July 2026	June operational policy retained and July filtering/monitoring amendments integrated. Short July amendment document superseded.

Prepared by	Chris Hill, CEO - 26 August 2026
Reviewed by	Chris Hill, CEO / Policy Owner - 26 August 2026
Approved by	Ian Balshaw, Chair of Trustees - DocuSign signature - 26 August 2026
Board sign-off recorded by	Chris Hill, CEO - Board Workspace - 26 August 2026
Next review due	Next review by August 2027, and sooner after legal, funder, service, serious incident or material risk change.
Earlier review trigger	Serious incident, significant near miss, premises change, major service change, significant technology change, commissioner requirement, or legal/local guidance update.

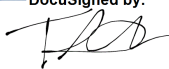
Approval and DocuSign signature record

Document status	Approved for launch and ready for DocuSign signature
Approval date	26 August 2026
Live from	1 September 2026
Next scheduled review	August 2027
Approval authority	Chair of Trustees, on behalf of the Board of Trustees
Live document library	Google Workspace
Superseded policy archive	Archive Workspace

Role	Name	Signature	Date
Chair of Trustees	Ian Balshaw	DocuSign signature	26 August 2026
Chief Executive Officer / Policy Owner	Chris Hill	DocuSign signature	26 August 2026

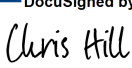
No further document text changes are required after DocuSign signature unless the Board, Chair, CEO or policy owner identifies an error before issue.

Ian

DocuSigned by:

3C7037478C9845A...

27-Aug-26 | 08:31 BST

Chris Hill

DocuSigned by:

9E01C80AC6FF40F...

26-Aug-26 | 17:02 BST