

IT-007 Online Safety and E-Safety Policy

Approved launch version. Live from 1 September 2026.

Element Society Online Safety and E-Safety Policy

Policy number IT-007 | Version July 2026

Policy number	IT-007
Status	Approved
Version	July 2026
Owner	Christopher Hill, Designated Safeguarding Lead and Online Safety Lead
Deputy DSL	Cleo Metcalf
Safeguarding Trustee	Ian Balshaw
Approval body	Chair of Trustees, on behalf of the Board of Trustees
Applies to	Education, alternative provision, HAF, youth work, outreach, online contact, one-to-one work, home visits, transport, trips and community activity
Next review due	Next review by August 2027, and sooner after legal, funder, service, serious incident or material risk change.

Use this policy with

Safeguarding Children Policy

Staff Code of Conduct and Safer Working Practice

Low-level Concerns and Whistleblowing Procedure

Data Protection, Information Sharing and Records Policy

AP safeguarding quick pull-out and AP operational annex

Behaviour, anti-bullying and physical intervention guidance

Photography, filming and media consent procedures

Educational Visits and Off-site Activity procedures

HR-025 Staff Acceptable Use Agreement

HR-PRIV-001 Staff Privacy Notice - Monitoring, Filtering and Device Use

IT-001 Data Protection Policy

IT-002 Information Security, Retention and Disposal Policy

IT-006 IT Systems Register

FM-001 Filtering and Monitoring Review Checklist

DPIA-FM-001 Filtering, Monitoring and Device Controls DPIA

Contents

1. Purpose

2. Scope

3. Legal and guidance framework

4. Principles

5. Roles and responsibilities

6. Online safety risks

7. Approved devices, accounts and platforms

8. Alternative provision and education arrangements

9. Youth work arrangements

10. Filtering and monitoring

11. Filtering and monitoring checks

12. Reporting online safety concerns

13. Responding to online safety incidents

14. Nude and semi-nude image-sharing

15. Child-on-child abuse and harmful online behaviour

16. Vulnerable children and additional risk

17. Curriculum and prevention

18. Parents, carers, schools and partners

19. Staff professional boundaries online

20. Images, filming, media and recordings

21. Generative AI and emerging technology

22. Third-party venues, networks, apps and providers

23. Records, tagging and theme review

24. Training and staff briefing

25. Policy review

- Appendix A. Staff acceptable use agreement
- Appendix B. Young person online safety agreement
- Appendix C. Filtering and monitoring summary checklist
- Appendix D. Approved platforms and systems register
- Appendix E. Online safety incident flow
- Quick action sheet

Recognise	Take seriously any online concern, harmful content, cyberbullying, unsafe contact, grooming concern, nude or semi-nude image-sharing, sexualised messaging, group chat dispute, online exploitation indicator, extremist content, misogyny, violent content, self-harm content, deepfake, AI misuse, repeated unsafe searches, or anything online that affects safety offline.
Respond	Stay calm. Make the situation as safe as possible. Reassure the child or young person that they have done the right thing by telling someone. Do not promise confidentiality. Do not investigate or ask leading questions. Do not view, copy, save, forward, print or share sexual images unless the DSL has agreed there is a clear safeguarding reason.
Record	Write a factual record on the same day. Include the date, time, platform/device if known, who was involved, what was seen or said, the child's own words where possible, what immediate action was taken, and who the concern was shared with.
Report	Report to the DSL or Deputy DSL straight away. In AP, also follow the AP same-day reporting route and notify the placing school or local authority through the agreed route where required.
Refer	The DSL or Deputy DSL will usually lead referrals to the Sheffield Safeguarding Hub, police, CEOP, Prevent/Channel, LADO, school, local authority, social care or other relevant agency. Any staff member 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.

1. Purpose

The purpose of this policy is to keep children and young people safe when using the internet, digital devices, social media, messaging, online platforms, images, video, AI tools and other technology as part of Element Society's work.

This policy sets out how Element Society:

keeps children and young people safe online and offline

sets clear expectations for staff, volunteers and young people

uses appropriate filtering and monitoring where Element manages devices or networks

responds to online safety concerns as safeguarding concerns where risk is present

manages professional boundaries online

uses images, video and digital evidence safely

supports children and young people to build digital resilience

works with parents/carers, schools, commissioners, social care, police and other agencies where required

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 all Element Society child-facing work, including:

education and alternative provision

Holiday Activities and Food delivery

detached, outreach and open-access youth work

youth club and community activity

one-to-one work

home visits

transport

educational visits and off-site activity

online or phone-based contact

use of Element devices, networks, accounts, apps or platforms

use of images, video, recordings and digital evidence

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:

Children Act 1989 and 2004

Education Act 2002, where relevant to education delivery

Working Together to Safeguard Children, current version

Keeping Children Safe in Education, current version, where Element delivers education or alternative provision

DfE filtering and monitoring standards for schools and colleges

DfE statutory guidance on alternative provision

Children Missing Education statutory guidance

Counter-Terrorism and Security Act 2015 and Prevent Duty guidance

Online Safety Act 2023

UK GDPR and Data Protection Act 2018

Information Commissioner's Office guidance on data protection, DPIAs and children's data

UKCIS guidance on sharing nudes and semi-nudes

Charity Commission safeguarding guidance for trustees

Sheffield safeguarding procedures, Sheffield Safeguarding Hub route, Sheffield LADO route and Sheffield alternative provision processes, where relevant

Where guidance changes, the current official version takes priority and this policy must be reviewed.

4. Principles

Element Society believes that:

children and young people should be safe online and offline

the online world offers opportunities for learning, connection, creativity and personal development

online activity can also create risk, including abuse, exploitation, bullying, grooming, harmful content, image-based abuse, radicalisation, fraud, coercion and misuse of AI

online and offline harm often overlap

technical controls support safeguarding, but they do not replace professional curiosity, supervision and safe relationships

children with SEND, trauma, care experience, exploitation risk, low confidence, mental health needs or communication needs may require additional support to stay safe online

safeguarding is everybody's responsibility

5. Roles and responsibilities

Board of Trustees

The Board retains overall responsibility for safeguarding and online safety governance. The Board must receive enough assurance to know that online safety arrangements are being used in practice, not only written down. The Board should be informed of significant online safety risks, serious incidents, system gaps and any major changes to filtering or monitoring arrangements.

Safeguarding Trustee

The Safeguarding Trustee provides oversight and challenge. The Safeguarding Trustee is the escalation route for concerns about the CEO/DSL and should be involved in assurance around online safety where risk is significant.

Designated Safeguarding Lead and Online Safety Lead

Christopher Hill is the DSL and Online Safety Lead. The DSL leads the safeguarding response to online concerns, reviews alerts or reports, identifies patterns, decides follow-up action, liaises with schools, commissioners and statutory agencies, and provides assurance that risks are being managed.

Deputy DSL

The Deputy DSL provides operational cover and may receive reports, advise staff, make referrals, review concerns and manage cases when covering or delegated.

Managers and project leads

Managers and project leads ensure that staff know this policy, follow approved communication routes, manage device and supervision expectations, record concerns, and escalate online safety risks immediately.

Operational digital or IT lead / contracted IT support

The operational digital or IT lead and/or contracted IT support maintains filtering and monitoring systems, completes technical checks, provides reports, records technical actions and works with the DSL and senior leaders to make prompt changes where gaps or new risks are identified.

All staff and volunteers

All staff and volunteers must supervise use, follow acceptable use and image-sharing rules, report concerns and system weaknesses, maintain professional boundaries online, and never rely solely on technical controls to keep children safe.

6. Online safety risks

Staff should be alert to online risks including:

cyberbullying and online harassment

group chat conflict brought into the setting

sexual messages or sexual harassment online

sharing of nude or semi-nude images

image-based abuse, deepfakes and AI-generated sexual images

pornography and exposure to sexual content

grooming, exploitation and unsafe contact from adults or unknown people

coercion, blackmail, threats, dares or harmful challenges

violent content, weapons content and content that escalates aggression

self-harm, suicide and eating disorder content

misogyny, hate content, racism and prejudice-based abuse

extremist content and radicalisation

fraud, scams, impersonation and account misuse

misuse of personal data, images, location information or contact details

misuse of generative AI or other digital tools

attempts to bypass filtering or monitoring, including VPNs and proxy services

Staff do not need proof before acting. A concern may come from a child, parent/carer, staff member, online alert, device log, school, commissioner, police, social care, peer report, behaviour change, attendance pattern, or professional judgement.

7. Approved devices, accounts and platforms

Only approved devices, accounts and platforms must be used for work with children and young people.

Approved routes currently include:

Element work email

Element work mobile call or text

WhatsApp from an Element work phone for approved youth work purposes only

approved project social media accounts

Element-owned devices for young people's online activity in AP/education

Element Wi-Fi and managed network access

Not approved:

personal phones for contacting young people

personal email accounts

personal social media accounts

private or hidden messaging with young people

personal cloud storage for young person information

unapproved education platforms or online learning tools

using staff personal devices to store images, videos, safeguarding information or young person personal data

WhatsApp with young people is only permitted for approved youth work purposes from an Element work phone. It is not used with AP pupils unless a separate risk-assessed and recorded arrangement has been authorised by the DSL.

WhatsApp with parents/carers is not currently a standard route. If introduced, it must be approved, risk assessed, recorded in the approved platforms register and covered by staff guidance.

8. Alternative provision and education arrangements

In AP and education delivery:

young people use Element-owned devices only for online activity

personal devices are not used by pupils for online learning or internet access during the AP day

pupils do not use personal mobile phones during the AP day; phones are handed in, securely stored or kept away according to the AP phone rule

staff directly supervise screen use

online activity must be linked to a planned, reasonable and supervised activity

staff must maintain visual awareness of screens where devices are in use

any concern must be reported to the DSL or Deputy DSL straight away

placing schools or the local authority must be informed through the agreed route where required

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 named safeguarding contact before delivery starts.

9. Youth work arrangements

In youth work settings, young people may have their own phones unless the activity risk assessment or behaviour expectations require limits.

Staff must challenge and respond to:

filming without consent

image-sharing without consent

bullying or harassment

sexual messages or sexual content

harmful content

unsafe contact or grooming concerns

racist, misogynistic, extremist or hateful content

online conflict affecting safety in the session

behaviour that places a young person or others at risk

Youth workers must use approved communication routes and maintain professional boundaries. They must not create private or exclusive online relationships with young people.

10. Filtering and monitoring

Where Element manages devices, networks, accounts or digital systems for education, AP, youth work or direct delivery with children and young people, appropriate filtering and monitoring must be in place.

Filtering is applied to all Element-owned internet-connected devices. Enhanced safeguarding monitoring is applied to devices used for education, AP, youth work or direct delivery with children and young people, where proportionate and technically available.

Current provision

Element is implementing Lightspeed as the dedicated filtering and monitoring system for Element-managed devices/accounts where configured. The DSL, senior leadership and IT support must complete and record a post-install suitability review by 31 August 2026 against current DfE filtering and monitoring expectations.

The Lightspeed review must confirm harmful content controls, alert routes, admin access, off-site protection, user/device visibility where available, retention and safeguarding escalation. Any gap must be recorded in IT-006 and FM-001 with an owner and deadline.

Filtering and monitoring must include a combination of:

technical filtering

technical monitoring or reviewable logs where available

harmful search/content alerts where available

staff supervision

clear behaviour expectations

incident recording

DSL review

termly checks and annual review

Technical controls do not replace professional vigilance. Staff must continue to supervise, check, challenge and report concerns.

11. Filtering and monitoring checks

Filtering and monitoring effectiveness must be checked at least termly and reviewed at least annually. Checks must also happen when:

Monitoring of staff use must be lawful, fair, transparent, necessary and proportionate. Staff must be informed through the Staff Privacy Notice and Staff Acceptable Use Agreement. A DPIA must be completed or reviewed before introducing new monitoring systems or materially changing monitoring arrangements.

a safeguarding risk is identified

a serious incident or near miss occurs

new devices are introduced

new apps, platforms or AI tools are introduced

the network or technical setup changes

delivery moves to a third-party venue or off-site location

there is a major software update

staff identify concerns about system weakness, overblocking or underblocking

Checks should record:

date of check

who completed the check

system checked

user group/profile checked

sample devices checked

blocked categories reviewed

alerts/reports reviewed

any concerning activity

any system gaps or limitations

actions taken

whether Lightspeed remains suitable

DSL sign-off

any escalation to SLT/trustees

Checks must consider whether filtering and monitoring cover:

age and ability of users

SEND and vulnerability

AP/education risk profile

off-site device use

AI-generated content

harmful searches

online sexual harm

self-harm and suicide content

extremism and terrorist content

misogyny and hate content

violent content

VPNs, proxy services and bypass attempts

safe search and browser settings

user/device identification

logs showing time, date and search/content where available

12. Reporting online safety concerns

Children, young people, parents/carers, staff and partners can report online safety concerns through:

any member of staff

DSL or Deputy DSL

project manager or AP lead

safeguarding email or agreed internal route

low-barrier reporting route: Tell us a worry through programme posters using a QR code, paper form or named staff route

complaints route where the concern is about service practice

whistleblowing route where the concern is about unsafe adult practice or poor organisational response

The Tell us a worry route is for low-barrier reporting by children, young people and parents/carers. It can be used to report worries about bullying, online safety, group chats, unsafe messages, images, threats, racism, sexual comments, grooming, harmful content or anything that makes someone feel unsafe.

The route must clearly say:

The Tell us a worry route is owned by the Deputy DSL and must be reviewed within 24 hours of receipt. Each programme must display the route through posters or an agreed equivalent.

This is not an emergency route. If someone is in danger now, tell a trusted adult straight away or call 999.

Anonymous reports must still be taken seriously. The DSL or Deputy DSL will review anonymous reports, consider immediate safety, check whether any child can be identified, and decide what action is needed. Where there is enough information to identify risk, the concern must be recorded and followed up through safeguarding procedures.

13. Responding to online safety incidents

Online safety incidents are treated as safeguarding concerns where there is risk of harm.

Staff must:

make the situation safe

listen calmly and take the concern seriously

avoid promising confidentiality

avoid investigating or asking leading questions

avoid viewing, copying, saving, forwarding, printing or sharing sexual images unless agreed by the DSL for a clear safeguarding reason

preserve evidence where safe and proportionate

record factually on the same day

report to the DSL or Deputy DSL straight away

escalate immediately if there is danger or delay

The DSL or Deputy DSL will:

review the concern

consider immediate safety and support

check relevant device/filtering/monitoring information where appropriate

consider whether parents/carers should be informed, unless doing so would increase risk or compromise social care or police processes

inform the placing school or local authority where relevant

refer to the Sheffield Safeguarding Hub, police, CEOP, Prevent/Channel, LADO or another agency where threshold is met or advice is needed

record actions, decisions and rationale

review patterns and prevention work

14. Nude and semi-nude image-sharing

Concerns involving nude or semi-nude images must be handled as safeguarding concerns.

Staff must not:

view images unless unavoidable or agreed by the DSL for a clear safeguarding reason

copy, save, print, forward, upload, screenshot or share images

ask a child to show images repeatedly

search a child's device unless authorised, trained and legally appropriate

investigate beyond what is necessary to keep children safe

Staff must:

reassure the child

avoid blame or shame

report immediately to the DSL or Deputy DSL

record factually

preserve relevant evidence only where safe and appropriate

follow DSL advice

The DSL will consider:

age and developmental stage

consent, coercion, pressure, blackmail or threats

whether an adult is involved

whether there is exploitation, grooming or abuse

whether images have been shared widely

whether police, CEOP or social care advice is required

support for the child whose image has been shared

support and safeguarding assessment for any child who shared or requested images

wider peer group impact

parent/carer involvement where safe

school/LA involvement where relevant

Children must be supported and safeguarded. They should not be automatically criminalised.

15. Child-on-child abuse and harmful online behaviour

Element recognises that children can harm other children online and offline. This includes bullying, sexual harassment, coercive control, sharing images, threats, intimidation, grooming behaviour between peers, group chat abuse, misogyny, racism, humiliation, blackmail, deepfakes and harmful sexual behaviour.

All reports must be taken seriously. Element will not dismiss online harm as banter, drama, growing up, or normal youth culture.

The child who has experienced harm must be listened to, supported and protected.

The child alleged to have harmed others must also be managed as a child who may have unmet needs, trauma, vulnerabilities or safeguarding needs. Staff should use factual language and avoid labelling before facts are established.

The DSL may put in place:

increased supervision

separate spaces or groupings

managed transitions

restricted unsupervised contact

adjusted timetable or activity access

separate arrival/departure arrangements

online/device restrictions

staff briefing on a need-to-know basis

risk assessment or safety plan

external referral or advice

Restorative work must only happen where it is safe, voluntary, age appropriate and agreed by the DSL. It must not be used where there is fear, coercion, sexual harm, exploitation, intimidation, significant power imbalance or statutory agency advice against it.

16. Vulnerable children and additional risk

Online safety risk assessments must consider:

SEND

communication needs

age and developmental maturity

trauma history

looked after status or care experience

exploitation risk

missing education or poor attendance

mental health needs

low confidence or isolation

previous abuse or harm

family context

peer dynamics

known triggers

online behaviour patterns

Controls may include:

closer supervision

restricted or supported device use

use of Element devices only

simple explanations and visual prompts

trusted adult check-ins

planned regulation breaks

parent/carer liaison where safe

information sharing with school/LA/social worker

adjusted curriculum

review of filtering and monitoring alerts

safety planning

17. Curriculum and prevention

Element will support children and young people to understand online safety through age-appropriate, needs-led and context-specific work.

This may include:

consent

boundaries

respectful relationships

online sexual harassment

nude and semi-nude images

pornography and harmful sexual attitudes

grooming and exploitation

group chat conflict

online bullying

racism and hate content

misogyny

violent content

extremism and radicalisation

harmful challenges

self-harm content

AI, deepfakes and misinformation

privacy, passwords and personal information

how to report worries

how to seek help safely

Content must be adapted for age, SEND, trauma, maturity, communication needs and vulnerability.

18. Parents, carers, schools and partners

Element will work openly and constructively with parents/carers, schools, commissioners and partner agencies where safe and appropriate.

Parents/carers should be given information about:

Element device and phone expectations

filtering and monitoring where relevant

online safety risks

how to report concerns

Tell us a worry anonymous route

who to contact

how online concerns will be managed

Parents/carers will normally be informed of concerns 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.

In AP or commissioned work, Element must share relevant, proportionate and necessary information with the placing school, local authority or commissioner through agreed routes.

19. Staff professional boundaries online

Staff and volunteers must maintain professional boundaries online.

Staff must:

use only approved work devices, accounts and platforms

record significant contact where required

use appropriate language

keep communication purposeful and proportionate

avoid private or exclusive relationships

report boundary slips immediately

self-report contact from a young person to a personal account

report concerns about staff online conduct through low-level concerns, whistleblowing or allegations procedures

Staff must not:

use personal social media to contact or follow young people

use personal phones for routine contact with young people

- send private or secret messages
- delete safeguarding-relevant messages without advice
- exchange personal images
- share inappropriate jokes, memes or content
- use online communication to avoid normal safeguarding or supervision routes

20. Images, filming, media and recordings

Images, video and recordings must only be taken, stored and shared in line with Element consent, safeguarding and data protection procedures.

Element will:

- use standard consent forms
- seek separate consent for internal evidence, funder reports, website, social media and press where required
- require parent/guardian consent for under-18s
- apply extra caution for looked after children, children at risk, children subject to legal restrictions, or children where public identification may increase risk
- ensure public posts are approved by Project Managers or senior leads
- avoid unnecessary personal data in captions
- remove images where consent is withdrawn unless there is a lawful reason to retain them
- store images securely
- never use images in a way that humiliates, exploits or increases risk

21. Generative AI and emerging technology

Children and young people do not currently use AI tools as part of Element delivery unless separately approved and risk assessed.

Staff may use AI for planning or administrative support, but must not enter identifiable child data, safeguarding details, personal information, confidential documents, images, names, addresses, health information, case details or anything that could identify a child, family, staff member or incident.

Any new use of AI with young people must be approved before use and must consider:

- safeguarding risks
- data protection
- bias and discrimination
- age appropriateness
- misinformation
- image generation and deepfake risk
- recording and supervision

parent/carer and commissioner expectations

22. Third-party venues, networks, apps and providers

Before using a third-party venue, network, app, platform or provider with children, staff must consider:

what children will access

who controls the system

whether filtering or monitoring is in place

whether Element devices remain protected

whether the platform stores personal data

whether children can message others privately

whether staff can supervise activity

whether images, recordings or chat are enabled

whether the provider has appropriate safeguarding and data protection arrangements

what will happen if an incident occurs

If safeguards are unclear or insufficient, the activity must not proceed until risks are reviewed and controls are agreed.

23. Records, tagging and theme review

Online safety concerns must be recorded in the safeguarding system or agreed safeguarding recording route.

Records should be tagged where possible so patterns can be identified. Useful tags include:

online safety

cyberbullying

group chat conflict

image sharing

nude/semi-nude images

grooming/exploitation

misogyny

racism/hate content

violent content

extremism

self-harm content

AI/deepfake

child-on-child abuse

harmful sexual behaviour

CSA concern

attendance/welfare concern

The DSL or Deputy DSL should review online safety patterns at least termly and use the findings to inform staff briefing, curriculum, supervision, risk assessment and filtering/monitoring controls.

24. Training and staff briefing

All staff and volunteers must receive online safety information as part of safeguarding induction and updates.

Training and briefings should cover:

this policy

professional boundaries online

approved devices and platforms

reporting routes

anonymous reporting

filtering and monitoring responsibilities

harmful content and online abuse

nude and semi-nude image-sharing

online sexual harassment

child-on-child abuse

exploitation and grooming

Prevent and radicalisation

AI, deepfakes and misinformation

recording and escalation

how to report technical weaknesses or staff conduct concerns

25. Policy review

This policy must be reviewed at least annually and sooner after:

a serious safeguarding incident

a serious near miss

a significant online safety incident

a major service change

a significant change in law or guidance

a commissioner requirement

a change in devices, filtering, monitoring, platforms or network arrangements

introduction of AI or new technology

findings from audit, inspection or quality assurance

The review should consider staff learning, safeguarding themes, technical reports, filtering and monitoring checks, incidents, complaints, commissioner feedback and lessons learned from practice.

Appendix A. Staff acceptable use agreement

This appendix is a quick online-safety summary only. Staff must also read and sign HR-025 Staff Acceptable Use Agreement, which sets the full acceptable use, monitoring, personal device and professional boundary requirements.

I will not use personal social media or personal messaging to contact young people.

I will not store images, personal data or safeguarding information on personal devices.

I will report online safety concerns immediately to the DSL or Deputy DSL.

I will report system weaknesses, filtering concerns or device concerns promptly.

I will not view, copy, save, forward, print or share nude or semi-nude images unless the DSL has agreed there is a clear safeguarding reason.

I will record significant online safety concerns factually and on the same day.

I will maintain professional boundaries online.

I will self-report any boundary slip, accidental contact or situation that could be misinterpreted.

I understand that misuse of technology may be managed through safeguarding, conduct, disciplinary, LADO or police routes depending on the concern.

Name:

Role:

Signed:

Date:

Appendix B. Young person online safety agreement

When I use Element devices, Wi-Fi or online activities, I agree to:

use the internet safely and respectfully

follow staff instructions

use only the device, app, site or activity staff have agreed

not try to bypass filters or controls

not search for harmful, violent, sexual or illegal content

not bully, threaten, pressure or embarrass others online

not share images of other people without permission

not ask for, send or share nude or semi-nude images

not use racist, sexist, homophobic, transphobic, misogynistic or hateful content

not contact unsafe people or share personal details online

ask staff for help if something worries me

report unsafe messages, images, group chats, grooming, bullying or harmful content

I understand that Element staff may supervise device use and that filtering and monitoring may be in place to help keep people safe.

Name:

Signed:

Date:

Appendix C. Filtering and monitoring summary checklist

This appendix is a summary prompt for this policy. The full review must be completed using FM-001 Filtering and Monitoring Review Checklist and saved in the safeguarding audit evidence folder.

Date of review:

Completed by:

DSL sign-off:

IT support involved:

System reviewed:

Current system: Lightspeed

Checks completed

Student/pupil filtering profile checked

Staff filtering profile checked

Guest/visitor access checked where relevant

Safe search checked

VPN/proxy bypass controls checked

Harmful content categories checked

Illegal child abuse material blocking checked where system allows

Terrorist/extremist content blocking checked where system allows

Adult content blocking checked

Misogyny/hate content categories checked

Violent content categories checked

Self-harm/suicide content categories checked

AI-generated/dynamic content limitations considered

Device logs reviewed

Alerts reviewed

High-risk alerts reviewed

Off-site device protection checked where relevant

New devices checked before use

Third-party venue/network risks reviewed

Issues/actions recorded

System remains suitable: Yes / No / Action required

If no or under review, escalation/action required:

Appendix D. Approved platforms and systems register

The approved platforms and systems register must be kept current. New systems, apps, AI tools or communication routes must not be used with children and young people until they have been checked and approved. The fuller system detail should also be recorded in IT-006 IT Systems Register.

System/platform	Approved use	Young people/data	Controls and evidence
Element work email	Professional communication by staff and authorised volunteers.	No direct young person access. Personal data may be involved.	Microsoft/tenant controls and audit where available. Covered by Data Protection Policy and Staff Privacy Notice.
Element work mobile call/text	Work communication and agreed contact by authorised staff.	Youth work/parent contact only where approved. Contact data and messages may be involved.	Device controls where available. Covered by Acceptable Use and Staff Privacy Notice.
WhatsApp from Element work phone	Approved youth work contact only. Not AP unless separately authorised.	Young people may be involved in youth work only. Messages and contact data may be involved. No safeguarding records stored here.	Phone/device controls. Significant contact recorded separately. Requires local risk assessment and staff guidance.
Project social media accounts	Project communication and engagement by authorised staff only.	Public engagement may involve young people. Images/video only with consent and approval.	Platform controls plus staff moderation. Media consent and data protection checks required.
Element-owned devices	Supervised AP/education and delivery activity.	Young people may use supervised devices. Personal data/images only where necessary and approved.	Filtering applied to all Element-owned devices. Enhanced monitoring where proportionate and technically available. Covered by DPIA-FM-001 and Staff Privacy Notice.
Lightspeed	Dedicated filtering and monitoring for Element-managed devices/accounts where configured.	Young people may be indirectly involved through supervised AP/education use; staff/device data may be involved.	Alerts reviewed as received through Lightspeed interface. DPIA-FM-001 approved and post-install suitability review due by 31 August 2026.
Generative AI tools	Staff planning/admin support only.	Not approved for direct young person use unless separately risk assessed. No identifiable child, family, staff, incident or safeguarding data.	No child monitoring function. Separate approval and DPIA if use changes.

Appendix E. Online safety incident flow

Concern identified

Immediate safety action

Report to DSL or Deputy DSL

Record same day

Check device/filtering/monitoring information where relevant

Consider child support and safety plan

Inform school/LA/commissioner where relevant

Inform parents/carers where safe and appropriate

Refer or seek advice where threshold is met: Sheffield Safeguarding Hub, police, CEOP, Prevent/Channel, LADO or other agency

Review pattern/theme

Update risk assessment, curriculum, supervision or technical controls

Sign-off and control record

Prepared by:

Role:

Date:

Reviewed by:

Role:

Date:

Approved by:

Role:

Date:

Board sign-off recorded by:

Date of board record:

Next review due:

Earlier review trigger:

Serious incident, significant near miss, major service change, commissioner requirement, major technology change, filtering/monitoring system change or legal/local guidance update.

Launch evidence and data governance locations

Record / register	Storage route
Staff policy acknowledgements	BreatheHR policy read records
Monitoring/filtering staff acknowledgement records	Google Forms / BreatheHR records as applicable
Data breach log	Google Forms
Subject access request log	Google Workspace
Processor/supplier register	Google Workspace
Retention schedule	Google Workspace
Tell us a worry route	Programme posters using QR code, paper form or named staff route; owned by Deputy DSL; reviewed within 24 hours

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