

CLEARSPACE LEARNING LTD

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Policy Information	Details
Company Registration	15950890
Policy Owner	Stuart Knox (Director/Designated Safeguarding Lead)
Version	1.1
Date of Issue	November 2025 · Last Updated: October 2026
Review Date	October 2027
Approved by	Stuart Knox, Director

1. POLICY STATEMENT

1.1 Our Commitment

Clearspace Learning recognises that technology and the internet are integral to modern education and life. We are committed to providing a safe digital environment where children can explore, learn, and develop digital literacy skills while being protected from online risks. This policy sets out how we keep children safe online, how we use technology responsibly in our provision, and how we teach children to navigate the digital world safely.

1.2 Purpose

This policy aims to:

- Protect children and young people from online harm
- Ensure safe and appropriate use of technology during sessions
- Educate children about online safety and digital citizenship
- Set clear expectations for staff use of technology
- Establish procedures for responding to online safety concerns
- Ensure compliance with safeguarding and data protection requirements

1.3 Scope

This policy applies to:

- All children accessing Clearspace Learning provision
- Stuart Knox and any future staff/tutors
- Parents and carers (guidance and partnership)
- Any use of technology during Clearspace sessions
- Online communication between staff and families
- Digital content created during sessions

2. THE ONLINE LANDSCAPE

2.1 Opportunities

Technology offers incredible educational opportunities:

- Access to information - vast resources for research and learning
- Creative tools - coding, design, music production, video editing
- STEM learning - programming, robotics, electronics
- Assistive technology - support for SEND and neurodivergent learners
- Communication - connecting with others, expressing ideas
- Motivation - engaging reluctant learners through digital media

2.2 Risks

Children can face risks online in four main areas:

CONTENT RISKS - Exposure to harmful material:

- Pornography and sexually explicit content
- Violence, gore, or disturbing images
- Hate speech, racism, or discriminatory content
- Self-harm or suicide content
- Eating disorder promotion ("pro-ana/mia")
- Fake news and misinformation
- Extremist or radicalising content
- Age-inappropriate material

CONTACT RISKS - Harmful interactions:

- Grooming for sexual abuse
- Online predators posing as children
- Cyberbullying and harassment
- Unwanted contact from strangers
- Radicalisation and extremist recruitment
- Peer pressure and negative influence

CONDUCT RISKS - Child's own behaviour:

- Sexting (sending/receiving sexual images)
- Cyberbullying others
- Sharing inappropriate content
- Illegal downloading or hacking
- Gambling or financial scams
- Excessive screen time affecting wellbeing

COMMERCE RISKS - Commercial exploitation:

- In-app purchases and online spending
- Gambling (including loot boxes in games)
- Financial scams and fraud
- Inappropriate advertising
- Identity theft

2.3 Vulnerability Factors

Neurodivergent children may face specific online risks:

- Social naivety - difficulty recognising manipulation or danger
- Literal thinking - may not understand sarcasm, deception, or hidden motives
- Intense interests - may be targeted in special interest communities
- Isolation - seeking connection online may make them vulnerable
- Impulsivity - may share information without considering consequences
- Trust - may trust online "friends" too readily

Our Approach: Tailored online safety education and vigilant supervision.

3. OUR ONLINE SAFETY PRINCIPLES

3.1 Core Principles

Education: We teach children to navigate the digital world safely

Empowerment: We give children skills to protect themselves

Protection: We create safe boundaries and supervision

Partnership: We work with parents to keep children safe online and offline

Proportionality: We balance safety with freedom to explore and learn

Resilience: We help children develop critical thinking and risk assessment

3.2 Age-Appropriate Approach

Primary Age (8-11):

- Simple, clear rules about online safety
- Adult supervision for all online activity
- Restricted access to appropriate content only
- Focus on: "Tell a trusted adult if something worries you"

Secondary Age (11-16):

- Developing critical thinking about online content
- Understanding privacy and digital footprint
- More independence with guidance and checking
- Focus on: "Think before you click/share"

Post-16:

- Supporting independent digital citizenship
- Understanding legal responsibilities online
- Career and further education use of technology
- Focus on: "Your online life is your real life"

4. USE OF TECHNOLOGY IN SESSIONS

4.1 When Technology is Used

Students may use technology during Clearspace sessions for:

Educational Activities:

- Research and information gathering
- Programming and coding (Python, Scratch, web development)
- Robotics and electronics projects
- Creative projects (video editing, music production, design)
- Assistive technology for SEND needs
- Educational games and apps
- Online learning platforms and AI tools (supervised; see Use of Artificial Intelligence in the Safeguarding Policy and the Data Protection and Privacy Policy)

Communication:

- Email to teachers or collaborators (supervised)
- Educational forums or communities (supervised)
- Video calls for remote sessions (with parent present)

4.2 Devices Used

Clearspace-Owned Devices:

- Laptop/tablet used by Stuart Knox for sessions
- Filtered and monitored internet access
- Antivirus and security software maintained
- Regular updates applied
- Screen visible to Stuart at all times

Student-Owned Devices:

- Students may use their own devices during sessions
- Parents responsible for device settings and parental controls
- We supervise use during sessions
- If inappropriate content discovered, reported to parent and DSL

4.3 Supervision Requirements

All technology use during Clearspace sessions is supervised:

Stuart Knox is present at all times when child uses technology

Screen is visible to supervising adult

Activity is for agreed educational purpose

If working online, browsing is monitored

Social media and gaming not accessed during sessions (unless specific educational purpose)

4.4 Internet Filtering and Monitoring

On Clearspace Devices:

- Internet content filtering in place (age-appropriate filters)
- Blocks pornography, violence, extremism, hate speech, gambling
- Search engine safe search enabled
- Browsing history monitored
- YouTube restricted mode enabled

On Student Devices:

- Parents responsible for parental controls and filtering
- We advise parents on appropriate settings
- We supervise use during sessions
- Inappropriate access stopped immediately and reported

5. ACCEPTABLE USE DURING SESSIONS

5.1 What Students MAY Use (With Supervision)

Educational Websites:

- Search engines (Google, DuckDuckGo) for research
- Wikipedia and educational reference sites
- BBC Bitesize, Khan Academy, educational platforms
- Coding sites (Scratch, Code.org, Repl.it)
- STEM resources (Tinkercad, Arduino tutorials, etc.)

Creative Tools:

- Video editing software (iMovie, Adobe, etc.)
- Music production software (GarageBand, Audacity)
- Graphic design tools (Canva, GIMP, Adobe)
- Programming IDEs and development tools

Communication (Supervised):

- Email for educational purposes
- Collaborative tools (Google Docs) for projects
- Video calls for remote sessions

Assistive Technology:

- Text-to-speech and speech-to-text
- Assistive apps for SEND needs
- Organisational and planning tools

5.2 What Students MAY NOT Use During Sessions

Social Media:

- TikTok, Instagram, Facebook, Snapchat, X/Twitter
- Unless specific educational purpose (digital citizenship lesson) with close supervision

Gaming:

- Online games and gaming platforms
- Unless specific educational purpose (game design lesson)

Inappropriate Content:

- Pornography or sexually explicit material
- Violence, gore, or disturbing content
- Hate speech or discriminatory content
- Self-harm or pro-eating disorder content
- Illegal content (piracy, hacking sites)

Personal Transactions:

- Online shopping
- Gambling or betting sites
- Financial transactions

Private Messaging:

- WhatsApp, Messenger, or other private messaging apps
- Unless supervised email for educational purpose

5.3 If Inappropriate Content is Accidentally Accessed

If a child accidentally accesses inappropriate content:

1. Stay calm - don't panic or overreact
2. Close/minimise immediately - don't let child continue viewing
3. Reassure child - "You didn't do anything wrong, accidents happen"
4. Don't investigate further - don't click through to see more
5. Report to DSL - Stuart Knox records incident
6. Inform parent - discuss what happened and reassure
7. Block site - add to filter if possible
8. Support child - brief conversation about what to do if it happens again

Do NOT:

- View the content yourself (if illegal e.g. child abuse images)
- Take screenshots (could be illegal if indecent images)
- Shame or blame the child
- Tell other children about it

6. ONLINE SAFETY EDUCATION

6.1 What We Teach

Online safety is embedded in our provision, not a one-off lesson. We teach:

SMART Rules:

- Safe - Keep personal information private
- Meet - Never meet online friends in person without adult
- Accepting - Don't accept files, messages from strangers
- Reliable - Not everyone online tells the truth
- Tell - Tell a trusted adult if worried

Privacy and Personal Information:

- What is personal information (full name, address, school, phone, photos)
- Why we keep this private online
- Privacy settings on apps and games
- Digital footprint - what you share stays online

Critical Thinking:

- Not everything online is true
- Recognising fake news and clickbait
- How to check sources
- Why people might lie or manipulate online

Healthy Relationships Online:

- Being kind online (digital citizenship)
- What cyberbullying is and how to respond
- Respecting others' privacy and feelings
- When to block, report, or tell an adult

Content and Copyright:

- Understanding copyright and intellectual property
- Not sharing others' work as your own
- Appropriate use of images and content
- Creative Commons and fair use

Screen Time and Wellbeing:

- Balancing online and offline life
- Recognising when technology use is unhealthy
- Sleep hygiene (screens before bed)
- Taking breaks and managing eye strain

6.2 Age-Specific Topics

For Younger Children (8-11):

- SMART rules
- Basic privacy (don't share your address)
- Tell an adult if worried
- Kind behaviour online

For Older Children (11-16):

- Sexting and sending nudes (illegal and harmful)
- Online grooming and CSE
- Social media pressures
- Extremism and radicalisation
- Healthy relationships and consent
- Digital footprint and future implications

For Post-16:

- Online reputation and employment
- Legal responsibilities (copyright, defamation, harassment)
- Critical media literacy
- Digital wellbeing and mental health

6.3 Resources We Use

- Thinkuknow (CEOP) - age-appropriate online safety resources
- Internet Matters - advice for parents and children
- NSPCC Online Safety - child-friendly resources
- Common Sense Media - reviews and guidance
- UK Safer Internet Centre - campaigns and resources

7. SPECIFIC ONLINE SAFETY ISSUES

7.1 Sexting and Sharing Nudes/Semi-Nudes

Definition: Creating, sharing, or possessing sexual images of under-18s.

The Law:

- Creating or sharing sexual images of under-18s is illegal (even if of yourself)
- Possession of indecent images of children is a serious criminal offence
- This applies even if the young person consents or shares voluntarily

Our Response:

If we become aware that a child has:

Received an unsolicited sexual image:

- Reassure child this is not their fault
- Advise not to forward or share
- Report to parent and police (if concerns about sender)
- Follow safeguarding procedures

Shared a sexual image of themselves:

- Immediate safeguarding concern
- Report to DSL (Stuart Knox)
- Contact parents (unless doing so would put child at risk)
- DSL assesses the incident using the UKCIS guidance "Sharing nudes and semi-nudes". Refer to children's social care (MASH) and/or the police at once where there is adult involvement, coercion or grooming, concerns about capacity to consent

(including because of SEND), unusual or violent content, sexual acts involving a child under 13, or immediate risk of harm

- Do NOT view the image or ask child to show it
- Support child with non-judgmental approach

Been involved in sharing others' sexual images:

- Serious safeguarding and criminal concern
- Report to DSL immediately
- Police involvement likely
- Follow child-on-child abuse procedures (see Safeguarding Policy, Recognising Abuse and Harm)

Prevention:

- Age-appropriate education about sexting
- Emphasis on: It's illegal, it's harmful, you can't control it once shared
- Empowering children to say no and report pressure

7.2 Cyberbullying

Definition: Using technology to deliberately upset, threaten, or humiliate someone.

Forms:

- Nasty messages or emails
- Posting embarrassing photos or videos
- Excluding someone from online groups
- Creating fake profiles to impersonate or mock
- Spreading rumours online
- "Trolling" (deliberately provoking reactions)

Our Response:

If a child reports being cyberbullied:

- Take it seriously - "It's just online" does NOT minimise harm
- Reassure child they did the right thing telling someone
- Record details (screenshots if possible)
- Contact parents of victim (and bully if both are Clearspace students)
- Report to commissioning school if bully attends there
- Support child to block, report, and protect themselves
- Follow Behaviour Management Policy procedures
- Refer to police if threats of violence or illegal content

If a Clearspace student is cyberbullying others:

- Safeguarding concern (about both bully and victim)
- Contact parents immediately
- Restorative conversation with child (why harmful, impact)
- Consequences as per Behaviour Policy
- Support to change behaviour
- Police involvement if serious

Prevention:

- Teaching digital citizenship and online kindness
- Empowering children to block, report, tell
- Creating culture where reporting is encouraged

7.3 Online Grooming and Child Sexual Exploitation (CSE)

Warning Signs:

- Child has secretive online relationships
- Receiving gifts or money from online contacts
- Using sexual language you wouldn't expect
- Older "boyfriend/girlfriend" they met online
- Secretive about device use or hides screen
- Receiving messages late at night

- Withdrawn or changes in behaviour

Our Response:

- Immediate safeguarding referral to MASH
- Contact parents (unless doing so increases risk)
- Preserve evidence (but don't investigate or view illegal content)
- Police involvement likely
- Follow CSE procedures in Safeguarding Policy (Recognising Abuse and Harm)

Prevention:

- Teaching about grooming tactics
- Emphasizing: "If it feels wrong, it probably is"
- Never meet online contacts in person
- Tell a trusted adult about online relationships

7.4 Radicalisation and Extremism (Prevent Duty)

Online radicalisation is when someone uses the internet to:

- Promote extremist ideologies
- Recruit individuals to extremist groups
- Encourage terrorist activity

Warning Signs:

- Accessing extremist websites or content
- Using extremist rhetoric or language
- Expressing support for extremist groups
- Increased secrecy about online activity
- Changing peer group (online or offline)
- Intolerance of difference

Our Response:

- Follow Prevent duty (Counter-Terrorism and Security Act 2015)
- Refer to Channel programme (deradicalisation support)
- Contact parents and commissioning school
- MASH referral if safeguarding concern
- Police involvement if immediate risk

Prevention:

- Critical thinking education about online content
- Building resilience to extremist narratives
- Promoting British values (democracy, rule of law, tolerance)
- Creating safe space to discuss difficult topics

7.5 Gaming and Online Communities

Risks:

- Contact with strangers in multiplayer games
- In-game chat used for grooming
- Exposure to inappropriate content
- Excessive spending (loot boxes, in-app purchases)
- Addiction and unhealthy gaming patterns

Our Approach:

- Gaming during sessions is rare (unless educational purpose)
- If used, we supervise and ensure privacy settings appropriate
- We educate about safe gaming (use of avatars, not sharing personal info)
- We advise parents on age ratings, parental controls, and healthy limits

Red Flags:

- Child mentioning online "friends" they've never met
- Secretive about gaming activity
- Spending long hours gaming (reported by parents)
- Changes in mood after gaming sessions

7.6 Social Media

Age Restrictions:

- Most social media platforms have minimum age of 13
- Some require 16+ (e.g., WhatsApp is officially 16+)
- Many children use platforms underage (often with parent knowledge)

Risks:

- Privacy concerns (personal information shared publicly)
- Cyberbullying and peer pressure
- Exposure to inappropriate content
- FOMO (fear of missing out) and mental health impacts
- Contact from strangers
- Permanent digital footprint

Our Approach:

- Social media not used during Clearspace sessions (generally)
- May be used for specific digital citizenship lessons (with close supervision)
- We educate about social media risks and privacy settings
- We support parents in managing their child's social media use

If Concerns Arise:

- Report inappropriate content using platform's reporting tools
- Screenshot evidence before reporting
- Contact parents
- Police if criminal content (threats, CSE, indecent images)

8. STAFF USE OF TECHNOLOGY

8.1 Professional Boundaries

All staff (current: Stuart Knox; future staff) must:

Use Technology Professionally:

- Use Clearspace Learning business email and phone for work
- Keep personal and professional technology separate
- Maintain appropriate boundaries in all digital communication

Communicate Appropriately:

- Contact parents via business phone (07986 622049) or email (info@clearspacelearning.com)
- Communication is professional, clear, and appropriate
- Respond to parents within 24 hours (working days)

Protect Children Online:

- Never have personal social media contact with students
- Never friend, follow, or connect with students on personal accounts
- Never share personal contact details with students
- Never engage in private messaging with students

NEVER:

- Use personal social media to contact students
- Share personal mobile number or email with students
- Engage in inappropriate communication with children online
- Share personal information or photos with students
- Accept friend requests from students on personal accounts
- Search for students on social media

8.2 Social Media Guidance for Staff

Personal Social Media:

- Staff responsible for own privacy settings
- Should be set to private/friends only

- Do not post anything that could bring Clearspace into disrepute
- Do not post anything inappropriate involving children
- Do not discuss Clearspace students online

Professional Social Media (if Clearspace has accounts):

- Managed by Stuart Knox only
- No student names or identifiable images without explicit parental consent
- Positive, professional content only
- Monitored and moderated

If Student Tries to Contact Staff on Social Media:

- Do not respond or accept request
- Report to DSL (Stuart Knox)
- Screenshot evidence
- Contact student's parents to advise

8.3 Use of Personal Devices

Mobile Phones:

- Staff may use personal phones during breaks
- Not used during sessions with children (except for business calls/texts)
- Photos/videos of children taken ONLY on Clearspace devices with consent
- Never taken on personal phones

Personal Laptops/Tablets:

- Should not be used for Clearspace work (use work devices)
- If necessary, must have antivirus, encryption, and password protection
- Clearspace data must not be stored on personal devices

8.4 Remote/Online Sessions

If sessions are delivered online (via Zoom, Teams, etc.):

Requirements:

- For under-18s: parent/carer present in the home during the online session (for safeguarding)
- Session recorded (with parental consent) for safeguarding purposes
- Both adult and child visible on camera
- Professional background/setting
- Appropriate dress code

Never:

- One-to-one online sessions with a child under 18 without a parent or carer present
- Sessions in bedrooms (use communal spaces)
- Communication outside of scheduled session times

9. PHOTOGRAPHY AND VIDEO

9.1 Taking Photos and Videos

Parental Consent Required:

- Written consent obtained before any photos/videos taken
- Consent specifies purpose and use
- Consent can be withdrawn at any time

When Photos/Videos MAY Be Taken (with consent):

- Recording educational activities for assessment
- Evidence of learning and progress
- Documenting projects (e.g., go-kart building, coding projects)
- Creating portfolios to share with parents

When Photos/Videos MUST NOT Be Taken:

- Without parental consent

- In private areas (bathrooms, changing rooms)
- If child objects or appears uncomfortable
- In states of undress
- In compromising situations
- Close-ups of upset or distressed children

9.2 Storage and Use

Storage:

- All images stored on encrypted, password-protected devices
- Access restricted to Stuart Knox only
- Cloud storage is UK-based and GDPR-compliant
- Images deleted when no longer needed or when child leaves provision

Use:

- Images used ONLY for agreed purpose (assessment, sharing with parents)
- NOT shared on social media or website without separate explicit consent
- NOT shared with other families or children
- NOT shared with external organisations without explicit consent

Sharing:

- Images shared with parents via secure methods (email, secure platform)
- Parents may share images of their own child as they wish
- Parents must not share images including other children

9.3 Children Taking Photos/Videos

During Sessions:

- Children may take photos/videos of their work (with supervision)
- Must not include other people without consent
- Supervision ensures appropriate content
- Stored on Clearspace device or child's device (with parent permission)

Selfies and Personal Images:

- Children may take photos of themselves during creative projects
- Parent consent and supervision required
- Education about online sharing and privacy

10. DATA PROTECTION AND ONLINE SAFETY

10.1 GDPR Compliance

All online data about children is handled in accordance with:

- UK GDPR and Data Protection Act 2018
- Our Data Protection and Privacy Policy
- Information Commissioner's Office (ICO) guidance

We ensure:

- Personal data is stored securely (encrypted)
- Access is restricted (password-protected, need-to-know basis)
- Data is not shared inappropriately online
- Parents' rights are respected (access, rectification, erasure)

10.2 Secure Communication

Email:

- Business email used for parent communication: info@clearspacelearning.com
- Sensitive information sent via secure methods
- Never send personal data to incorrect recipients

Cloud Storage:

- UK-based, GDPR-compliant providers only

- Password-protected and encrypted
- Two-factor authentication enabled

Video Calls:

- Secure platforms only (Zoom, Teams with security settings)
- Passwords required for sessions
- Waiting rooms enabled

11. RESPONDING TO ONLINE SAFETY CONCERNS

11.1 Types of Concerns

Immediate Safeguarding Concerns:

- Child viewing or sharing indecent images
- Evidence of online grooming or CSE
- Child being contacted inappropriately by adult
- Sexting or sexual harassment
- Threats of violence or self-harm
- Illegal content (terrorism, child abuse, hate crime)

Non-Urgent Concerns:

- Child accidentally accessed inappropriate content
- Low-level cyberbullying (name-calling)
- Excessive screen time concerns
- Parental concerns about child's online activity

11.2 Procedures for Staff

If you have an online safety concern:

STEP 1: Assess Urgency

- Is this an immediate safeguarding concern?
- Is a child at risk right now?

STEP 2: Preserve Evidence (if safe to do so)

- Screenshot concerning content (if legal and safe)
- Do NOT view illegal content (e.g., child abuse images)
- Do NOT forward or share concerning content
- Note: URL, platform, username, date/time, what you saw

STEP 3: Report to DSL

- Contact Stuart Knox immediately: 07986 622049
- Provide details and evidence
- Do NOT investigate further yourself

STEP 4: DSL Takes Action

- Follows safeguarding procedures (Safeguarding Policy: What To Do If You Have A Concern)
- Reports to MASH if safeguarding concern
- Reports to police if criminal content
- Reports to CEOP if online abuse: www.ceop.police.uk/safety-centre
- Contacts parents (unless increases risk)
- Reports to platform (using platform reporting tools)

STEP 5: Support Child

- Non-judgmental approach
- Reassure child they did right thing reporting
- Follow welfare and support procedures

11.3 Reporting Illegal Content

Child Abuse Images:

- DO NOT view, forward, or save

- Report to police immediately: 999 or 101
- Report to Internet Watch Foundation: www.iwf.org.uk
- Follow safeguarding procedures

Terrorism or Extremism:

- Report to police anti-terrorism hotline: 0800 789 321
- Report online via gov.uk/ACT
- Follow Prevent procedures

Other Illegal Content:

- Report to police if criminal (threats, harassment, hate crimes)
- Use platform reporting tools
- CEOP for online sexual abuse/exploitation

11.4 Supporting Children After Incidents

Emotional Support:

- Validate feelings ("That must have been scary/upsetting")
- Reassure ("You did the right thing telling someone")
- Normalise reactions
- No judgment or blame

Practical Support:

- Blocking/unfriending concerning contacts
- Adjusting privacy settings
- Reporting content on platforms
- Taking a break from devices if needed

Education:

- What to do if it happens again
- How to protect themselves
- Understanding it wasn't their fault

Ongoing Monitoring:

- Check in regularly
- Watch for signs of distress
- Liaise with parents and school

12. WORKING WITH PARENTS

12.1 Partnership Approach

We believe parents are children's first educators in online safety. We work in partnership by:

Sharing Information:

- This policy available to all parents
- Online safety tips and resources shared regularly
- Updates on new risks or platforms

Supporting Parents:

- Advice on parental controls and settings
- Signposting to resources (Internet Matters, NSPCC, Thinkuknow)
- Honest conversations about children's online activity

Encouraging Communication:

- Parents welcome to discuss concerns
- We share concerns with parents promptly
- Joint approach to managing online safety

12.2 Advice for Parents

We encourage parents to:

Have regular conversations about online activity

Know what games, apps, and platforms child uses

Set age-appropriate parental controls
Keep devices in communal areas (not bedrooms)
Set screen time boundaries
Model healthy technology use
Know who child is talking to online
Trust instincts - if it feels wrong, investigate

Red Flags for Parents:

- Secretive about device use
- Excessive screen time
- Changes in mood after online activity
- Receiving gifts from unknown people
- Using sexual language unexpectedly
- Withdrawing from family/friends

12.3 Useful Resources for Parents

Parental Control Guides:

- Internet Matters: www.internetmatters.org/parental-controls
- NSPCC Online Safety: www.nspcc.org.uk/keeping-children-safe/online-safety

Age-Appropriate Advice:

- Thinkuknow: www.thinkuknow.co.uk (resources for different ages)
- Net Aware: www.net-aware.org.uk (guide to social networks and apps)

Reporting Concerns:

- CEOP: www.ceop.police.uk/safety-centre (report online abuse)
- UK Safer Internet Centre: reportharmfulcontent.com
- Internet Watch Foundation: www.iwf.org.uk (report child abuse images)

13. TRAINING AND AWARENESS

13.1 Staff Training

All staff receive:

On Induction:

- This Online Safety Policy
- Safeguarding procedures (including online abuse)
- Acceptable use expectations
- How to report concerns

Annually:

- Online safety update training
- New platforms and risks
- Case studies and learning
- Policy review

Ongoing:

- Updates on emerging risks
- Platform-specific guidance
- Government guidance and legislation changes

13.2 DSL Training

Stuart Knox (DSL) receives specific training on:

- Online safeguarding concerns (grooming, CSE, radicalisation)
- Responding to sexting incidents
- Legal framework around online abuse
- Working with police and CEOP

14. LEGISLATION AND GUIDANCE

This policy is informed by:

Legislation:

- Children Act 1989 and 2004
- Education Act 2002
- Communications Act 2003 (malicious communications)
- Sexual Offences Act 2003 (indecent images)
- Serious Crime Act 2015 (sexting)
- Counter-Terrorism and Security Act 2015 (Prevent duty)
- Data Protection Act 2018 and UK GDPR

Statutory Guidance:

- Keeping Children Safe in Education 2026 (online safety)
- Working Together to Safeguard Children 2023
- Searching, Screening and Confiscation 2018
- Prevent Duty Guidance 2021

Non-Statutory Guidance:

- Teaching Online Safety in Schools (DfE)
- Education for a Connected World Framework
- UKCIS guidance (UK Council for Internet Safety)
- CEOP Thinkuknow resources

15. REVIEW AND MONITORING

15.1 Policy Review

This policy will be:

- Reviewed annually (October 2027)
- Updated in response to incidents or new risks
- Updated when new platforms or technology emerges
- Shared with parents and commissioning schools

15.2 Incident Monitoring

All online safety incidents are:

- Recorded confidentially
- Reviewed for patterns or trends
- Reported to relevant authorities as required
- Used to improve practice and education

16. RELATED POLICIES

This policy should be read alongside:

- Safeguarding and Child Protection Policy (Recognising Abuse and Harm; Working Safely; Information Sharing and Confidentiality)
- Data Protection and Privacy Policy (including Use of Artificial Intelligence)
- Behaviour Management Policy (cyberbullying)
- SEND Policy (vulnerability and assistive technology)
- Photography and Consent procedures (in Safeguarding Policy)

17. KEY CONTACTS

17.1 Internal Contacts

Designated Safeguarding Lead:

- Stuart Knox: 07986 622049
- Email: info@clearspacelearning.com

To Report Online Safety Concerns:

- DSL (above) immediately
- Out of hours: Follow safeguarding procedures

17.2 External Contacts

CEOP (Child Exploitation and Online Protection):

- Report online abuse: www.ceop.police.uk/safety-centre

Internet Watch Foundation:

- Report child abuse images: www.iwf.org.uk
- Hotline: 0800 347 8000

NSPCC:

- Helpline: 0808 800 5000
- Email: help@nspcc.org.uk

Police:

- Emergency: 999
- Non-emergency: 101
- Anti-terrorism hotline: 0800 789 321

Local Authority Safeguarding:

- See contact numbers in Safeguarding Policy (Appendix G, Contact Directory)

POLICY APPROVAL

This Online Safety and Acceptable Use Policy has been reviewed and approved by:

Stuart Knox

Director and Designated Safeguarding Lead

Clearspace Learning Ltd

Date: November 2025 (updated October 2026)

Next Review Date: October 2027

Company Registration: 15950890

Contact: info@clearspacelearning.com | 07986 622049

Website: www.clearspacelearning.com

APPENDIX A: ACCEPTABLE USE AGREEMENT FOR STUDENTS

I agree to use technology safely and responsibly during Clearspace Learning sessions:

- I will only use technology for agreed educational activities
- I will not access inappropriate websites or content
- I will not share personal information online
- I will tell Stuart immediately if I see something that worries me
- I will be kind and respectful online
- I will not cyberbully or be mean to others online
- I understand that rules apply online just like they do offline

I understand that:

- Stuart will supervise my technology use
- My parents will be informed if I break these rules
- I may lose technology privileges if I misuse devices

Student Name: _____

Signature: _____

Date: _____

Parent/Carer Name: _____

Signature: _____

Date: _____

APPENDIX B: TOP TIPS FOR ONLINE SAFETY

For Children:

- 1. Keep personal info private (full name, address, school, phone)**
- 2. Tell a trusted adult if something online worries you**
- 3. Think before you click or share**
- 4. Be kind online - treat others how you want to be treated**
- 5. Not everyone is who they say they are online**
- 6. Never meet online friends without telling a trusted adult**
- 7. Block and report anyone who makes you uncomfortable**
- 8. Remember: If it feels wrong, it probably is**

For Parents:

- 1. Talk regularly about what your child does online**
- 2. Use parental controls appropriate for your child's age**
- 3. Keep devices in communal areas (not bedrooms overnight)**
- 4. Know their passwords (for younger children)**
- 5. Check privacy settings on apps and games**
- 6. Set screen time limits and stick to them**
- 7. Model healthy use - put your phone down too!**
- 8. Trust your instincts - investigate concerns**