SG Policy Appendix 5

Online Safety Policy

'Safe, Responsible and Professional Online Behaviours'

Scope

This policy applies to all members of the Reflections Training Academy community (including staff, learners, volunteers, parents and carers, visitors and community users) who have access to and are users of academy digital systems, both in and out of the academy. It also applies to the use of personal digital technology on the academy network (where allowed).

It outlines the commitment of Reflections Training Academy to safeguard members of our community in accordance with statutory guidance and best practice. The academy should be aware of the legislative framework under which this policy and guidance has been produced.

Reflections Training acknowledges the benefits and opportunities which technology can offer to teaching and learning. It encourages us to enhance our skills and promote achievement. However, it is also acknowledged that the accessible and global nature of the internet and various technologies available means constant monitoring and awareness of potential risks and challenges associated with such use.

Our approach is to ensure learners are safeguarded from potentially harmful and inappropriate online material through the implementation of safeguards and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance; implementation of our associated policies. This policy should be read in conjunction with:

- Safeguarding Policy and Staff Safeguarding Code of Conduct
- Prevent Policy
- KCSiE and Working Together to Safeguard Children, 2026
- Acceptable Use Procedures
- Legislative Guidance

Policy Development, Monitoring and Review

This Online Safety Policy has been developed and updated by the Safeguarding Team, considering current legislation, statutory guidance, including Keeping Children Safe in Education (KCSIE), and recognised best practice.

Responsibility for monitoring the implementation and effectiveness of this policy rests with the Safeguarding Team, with support from the IT team where appropriate. Monitoring will take place on a regular basis, and a summary of findings and any recommended actions will be reported to the Senior Management Team, Directors and Governors (or equivalent governing body) at least annually.

This policy will be reviewed annually as part of the organisation's policy review cycle, or sooner where necessary to reflect changes in legislation, statutory guidance, emerging technologies, online safety risks, or following a significant online safety incident.

Any serious online safety incidents will be managed in accordance with the safeguarding procedures and, where appropriate, reported to the relevant Local Authority, external safeguarding partners, and/or the Police.

Senior Manager Divisional Safeguarding/Prevent (DSL)

Reflections Training Academy

This policy was considered and adopted by the following Directors:

Clare Barrett

Company Managing Director

Lucy Agnew

Divisional Director of Training

Phil Davis

Director of Bristol Training Academy

Kate Sperring

Director or Next Level Training

Version 21 July 2026

Policy Owner	Director Sign Off	Details of Update	Date of Update	Version Number
Jason Timms	Lucy Agnew	Policy review & update	28/11/2019	13
Jason Timms	Lucy Agnew	Policy renames and rewrite	29/06/2020	14
Jason Timms	Lucy Agnew	Policy review & update	21/04/2021	15
Jason Timms	Lucy Agnew	Policy review & KCSIE 2021 update	17/09/2021	16
Jason Timms	Lucy Agnew	Policy review & KCSIE 2022 update	16/08/2022	17
Jason Timms	Lucy Agnew	Policy review & KCSIE 2023 update	25/08/2023	18
Suzanne Sewell	Lucy Agnew	Policy review & KCSIE 2024 update/360safe self-review tool/other legislative guidance	01/04/2025	19
Suzanne Sewell	Lucy Agnew	Policy Review KCSIE 2025	12/08/2025	20
Suzanne Sewell	Lucy Agnew	Policy Review KCSIE 2026	29/07/26	21
Next update:		July 2027		

The academy will monitor the impact of the policy using:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Reviews of the effectiveness of the filtering systems
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Learners, Parents/carers, Staff

5. Online Safety - Filtering and Monitoring Procedures

In fulfilling our responsibility to safeguard and promote the welfare of children and young people, and to provide a safe and secure learning environment, Reflections Training Academy/Next Level takes all reasonable and proportionate steps to minimise learners' exposure to harmful or inappropriate online content when using Academy IT systems.

All learner-accessible Academy IT systems are protected by content filtering that meets or exceeds the Department for Education's (DfE) Filtering and Monitoring Standards. These systems are designed to monitor, identify, and where appropriate, block access to websites and online content that are known to be illegal, harmful, inappropriate, or present a safeguarding risk. Filtering and monitoring measures are regularly reviewed to ensure they remain effective, proportionate, and responsive to emerging online risks.

Filtering, Monitoring and Safe Use of Technology

LanSchool monitoring software is deployed across learner-accessible IT systems to support the monitoring of online activity. The system generates alerts relating to predefined keywords, “activity indicative of potential safeguarding concerns” and attempts to access inappropriate or potentially harmful content. These alerts are monitored by the IT team and escalated to the Safeguarding Team where

appropriate. Any safeguarding concerns identified through monitoring are managed in accordance with the organisation's safeguarding procedures and recorded on MyConcern.

To ensure the effectiveness of our filtering arrangements, learner-accessible IT systems and servers are tested twice yearly using the SWGfL Test Filtering service. This testing evaluates the effectiveness of filtering against recognised lists, including the Internet Watch Foundation (IWF) list of child sexual abuse material, UK Counter Terrorism Internet Referral Unit (CTIRU) content, and other categories of illegal or harmful content. This includes child sexual abuse material, terrorist-related content, pornography and content containing profane or inappropriate language.

We recognise that many learners access the internet using personal mobile devices and mobile data, which operate outside the Academy's filtering and monitoring systems. Consequently, all staff remain vigilant to learners' online activity while on Academy premises and take appropriate action where concerns arise.

The Learner Acceptable Use of Technology Agreement sets out clear expectations for the safe and responsible use of technology. It explains learners' responsibilities when using Academy IT systems, supports our commitment to safeguarding and the Prevent Duty, and identifies acceptable and unacceptable use. Any misuse of technology will be managed in accordance with the organisation's behaviour, disciplinary and safeguarding procedures.

The use of technology and digital platforms is regularly reviewed to identify any emerging safeguarding risks. Concerns relating to inappropriate or risky online behaviour are treated as safeguarding matters and managed through the organisation's safeguarding procedures.

For all remote and online learning, staff and learners are required to comply with the Remote and Online Learning Code of Conduct, the Learner Acceptable Use of Technology Agreement (Appendix 5), and the requirements set out in this Online Safety Policy.

All staff and learners receive online safety education as part of their induction and ongoing training. This includes awareness of the four key areas of online risk: content, contact, conduct and commerce, together with guidance on recognising, responding to and reporting online safety concerns.

Further guidance can be found within this Online Safety Policy and in Keeping Children Safe in Education (2026), paragraphs 157–175.

5b. Online Safety Misinformation, Disinformation and Conspiracy Theories

As part of our statutory duty under KCSiE, we recognise the growing safeguarding risk posed by online spread of misinformation (false or misleading information shared without harmful intent) and disinformation (false information shared with intent to deceive). We are committed to helping learners develop digital resilience, critical thinking, and the ability to safely navigate online spaces.

This includes:

· Educating learners, through the curriculum, on how to identify, question and challenge misinformation and disinformation.

· Training all staff to recognise the safeguarding risks linked to harmful or radicalising content shared online, including health-related misinformation, extremist narratives, and conspiracy theories.

· Ensuring our filtering and monitoring systems are regularly reviewed and updated to reflect emerging online risks

· Acting promptly when pupils are found to be sharing, influenced by, or harmed by false online content that may affect their safety, wellbeing, or the safety of others

· Raising awareness of online risks and promotion of safe, informed use of digital media within the home or workplace.

Where concerns are linked to misinformation, disinformation, or harmful content, these will be managed in line with our safeguarding procedures and, where necessary, referred to the Designated Safeguarding Lead/Officer (DSL/DSO), external agencies or prevent.

Online Safety Policy Expectations, Actions and Communication

- Sets expectations for safe and responsible use of digital technologies for learning, administration and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the academy and how they should use this understanding to help safeguard learners in the digital world
- Describes how the academy will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Supplemented by a series of related acceptable use agreements
- Made available at staff inductions
- Published on the Reflections Training Academy/Next Level Website
- Defined what is regarded as acceptable/unacceptable use and can be found in the relevant Acceptable Use Agreements *(document outlining expectations on the responsible use of technology by its user)*
- Both policy and AUA and will be communicated/re-enforced through:
    - Learner Induction Process
    - Employer Safeguarding Your Apprentice Guidance and Employer Update Workshops
    - Staff Induction and any related policies and procedures

- Staff Safeguarding Code of Conduct
- Posters/notices in areas of technology use
- Communication with employers, parents and carers (as needed)
- Built into wider skills element of all academies offered programmes
- Website

Responsibilities

It is important that all members of the community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. Whilst this is a team effort, the following outline responsibilities of individuals and groups:

Directors and Governors

The Board of Directors and Governors are responsible for providing strategic oversight of safeguarding and online safety, ensuring that a strong safeguarding culture is embedded throughout the organisation. Their responsibilities include:

Ensuring that effective arrangements are in place to safeguard and promote the welfare of children and young people, including robust online safety measures.

Delegating day-to-day responsibility for online safety to the Designated Safeguarding Lead/Officer (DSL/DSO), in accordance with the requirements of Keeping Children Safe in Education (KCSIE).

Being aware of the procedures to be followed where a serious online safety allegation or incident involves a member of staff.

Ensuring that the DSL/DSO and other relevant staff have sufficient time, resources, authority and appropriate training to fulfil their safeguarding and online safety responsibilities effectively, including delivering training and guidance to colleagues where required.

Ensuring appropriate filtering and monitoring systems are in place to support the safe use of technology and to identify potential safeguarding concerns.

Receiving regular reports from the DSL/DSO on online safety, filtering and monitoring, safeguarding trends, and any significant incidents, to enable effective governance and oversight.

Ensuring that all staff receive safeguarding and child protection training, including online safety, as part of their induction and through regular updates. This training must include an understanding of staff roles and responsibilities in relation to filtering and monitoring.

Ensuring that learners are taught about safeguarding, including how to stay safe online, as part of an effective curriculum and wider safeguarding approach.

Reviewing the Department for Education's Filtering and Monitoring Standards and seeking assurance from the DSL/DSO, IT staff and RAKATA (external IT service provider) that appropriate systems and processes are in place and remain effective.

Supporting and enabling the DSL/DSO to work collaboratively with IT staff and service providers to ensure that filtering and monitoring arrangements are effective, proportionate, regularly reviewed, and responsive to emerging safeguarding risks.

Designated Safeguarding Lead (DSL) with Support from the Online Safety Team (IT Lead/Designated Safeguarding Officer)

The Designated Safeguarding Lead (DSL) has overall operational responsibility for online safety as part of their wider safeguarding role and is supported by the Online Safety Team, including the IT Lead and Designated Safeguarding Officer (DSO). Their responsibilities include:

Leading on all aspects of online safety and ensuring effective safeguarding arrangements are in place across Reflections Training/Next Level.

Maintaining up-to-date knowledge through appropriate safeguarding and online safety training, including emerging technologies, online risks, filtering and monitoring requirements, and relevant statutory guidance.

Meeting regularly with Directors and the Senior Management Team to review online safety arrangements, safeguarding concerns, filtering and monitoring reports, trends, and any significant incidents.

Attending Board and Governor meetings, as directed and where appropriate, to provide updates on safeguarding and online safety matters.

Receiving, assessing and managing reports of online safety incidents, determining whether concerns meet the threshold for referral to external agencies, and ensuring all incidents are recorded and managed in accordance with safeguarding procedures.

Working with programme leads to ensure that online safety education is planned, mapped, embedded and evaluated throughout the learner journey, taking account of learners' individual needs and vulnerabilities.

Ensuring that clear procedures are communicated and followed in the event of an online safety incident.

Developing and coordinating Reflections Training/Next Level programme of online safety training and continuing professional development (CPD) for staff, together with learner education and wider skills activities.

Ensuring that all staff receive appropriate safeguarding and online safety training, including an understanding of their responsibilities in relation to filtering, monitoring and the safe use of technology.

Ensuring that learners are taught how to keep themselves and others safe online through an age-, stage- and needs-appropriate programme of education that reflects emerging risks and individual vulnerabilities.

Working collaboratively with the nominated Online Safety Team (OST) lead, IT staff and RAKATA (external IT service provider) to review the effectiveness of filtering and monitoring systems at least annually, and more frequently where necessary.

Ensuring that filtering and monitoring reviews assess the effectiveness of controls across all learner-accessible, internet-connected devices and relevant learning environments.

Maintaining accurate records of all filtering and monitoring reviews, including the date of the review, systems and devices tested, locations covered, issues identified, actions taken, and confirmation that any required improvements have been completed.

Online Safety Team (supporting role) – DSO/IT Lead

- Works closely with DSL on a day-to-day basis
- Monitor internal systems and make DSL aware of any potential child protection concerns and ensure these are logged to inform future online safety developments
- Support policy review and updates
- Support and promote an awareness of and commitment to online safety education/awareness across the academy and beyond
- Support any staff CPD awareness of: Content, Contact, Conduct and Commerce.

All Staff

All staff have a responsibility to safeguard learners and promote safe, responsible and appropriate use of technology. Online safety is recognised as a core element of safeguarding, and all staff are expected to:

Maintain an up-to-date awareness of online safety issues, emerging technologies, current risks and trends, and comply with this Online Safety Policy and associated procedures.

Read, understand and comply with the Staff Safeguarding Code of Conduct, Staff Acceptable Use Agreement and all relevant safeguarding, data protection and information security policies.

Follow all relevant legislation and statutory guidance, including Keeping Children Safe in Education (KCSIE), the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Recognise that online safety concerns are safeguarding concerns and report any suspected or actual incidents immediately to DSL/DSO or Jordan Cross (IT Lead), in line with the Reflections Training/Next Level safeguarding procedures.

Use Academy devices, systems and communication platforms appropriately and ensure that all professional communication with learners, parents, carers and external partners is conducted through authorised Academy systems and processes.

Supervise and monitor learners' use of digital technologies during learning sessions and Academy activities, ensuring compliance with the Learner Acceptable Use Agreement and responding promptly to any concerns.

Ensure learners understand safe and responsible online behaviour, digital literacy, research skills, plagiarism, copyright and intellectual property requirements.

Only direct learners to appropriate online resources that have been reviewed for suitability and remain vigilant to inappropriate material that may be encountered during internet searches.

Ensure that internet access for learning activities takes place using Academy-provided devices and in accordance with Reflections Training/Next Level policies.

Follow national safeguarding guidance and Reflections Training/Next Level procedures when delivering remote or online learning.

Promote a zero-tolerance approach to online bullying, sexual harassment, exploitation, discrimination, hate-related behaviour, radicalisation, extremist content and all forms of online abuse.

Comply with the Academy cyber security requirements by protecting passwords, safeguarding login credentials, locking devices when unattended and never sharing accounts or using generic login details.

Understand the purpose and limitations of the Academy filtering and monitoring systems, recognising that no technical solution is completely effective and that professional vigilance remains essential.

Use only Academy-approved Artificial Intelligence (AI) services that have been appropriately risk assessed and meet Academy security, safeguarding and data protection requirements.

Understand both the benefits and risks associated with AI technologies, including the potential for inaccurate, biased or inappropriate outputs. AI should support, but never replace, professional judgement. Staff remain responsible for verifying AI-generated content, critically evaluating its accuracy and ensuring that all decisions affecting learners or colleagues are made by an authorised member of staff.

Where AI tools are used with learners, ensure that they incorporate appropriate safeguards to reduce access to harmful or inappropriate content and that staff understand the capabilities and limitations of any embedded filtering or monitoring mechanisms.

IT Provider

RKATA (IT Provider) plays a key role in supporting Reflections Training/Next Level safeguarding responsibilities by maintaining secure, reliable and effective technology systems. In partnership with the Designated Safeguarding Lead (DSL), Designated Safeguarding Officer (DSO) and (OST), the IT Provider will:

Be familiar with and comply with the Academy's Online Safety Policy, Technical Security Policy and all relevant safeguarding and information security requirements.

Ensure that the Academy's technical infrastructure is secure, resilient and protected against unauthorised access, misuse, cyber threats and malicious attack.

Ensure that systems and services meet, as a minimum, the Department for Education's (DfE) Digital and Technology Standards and other relevant statutory guidance relating to online safety, filtering and monitoring.

Maintain secure user account management processes, ensuring that access to networks, systems and devices is appropriate, controlled and regularly reviewed.

Work proactively with Academy Top Team to evaluate and implement new technologies that strengthen cyber security, online safety and safeguarding arrangements.

Ensure that anti-malware and endpoint protection software is installed, maintained, regularly updated and operational on all compatible devices.

Ensure that operating systems, Microsoft 365 services (including OneDrive), applications and security patches are regularly monitored and updated to maintain security and system performance.

Configure, maintain and regularly review filtering and monitoring systems to ensure they provide effective protection against illegal, harmful and inappropriate online content and activity, while remaining proportionate to the needs of learners and staff.

Agree filtering categories, monitoring thresholds and alerting arrangements in collaboration with the DSL, DSO and Academy leadership, ensuring that safeguarding priorities are appropriately reflected.

Support the Academy in meeting the expectations of Keeping Children Safe in Education (KCSIE), the DfE Filtering and Monitoring Standards, the DfE guidance on Generative AI: Product Safety Expectations, and recognised sector best practice.

Ensure that Academy Top Team and relevant safeguarding staff understand the capabilities and limitations of filtering and monitoring systems, including the challenges associated with monitoring dynamic, personalised and AI-generated content.

Promptly report any actual or suspected cyber security incident, system vulnerability, data breach or safeguarding-related technical concern to the DSL, DSO, IT Lead and/or Academy Directors, enabling timely investigation, risk assessment and appropriate action.

Support the annual review of filtering and monitoring arrangements by providing technical evidence, system reports and recommendations for continuous improvement.

Learners

Learners are expected to use digital technologies safely, responsibly and in accordance with Academy expectations. They play an important role in maintaining a safe learning environment for themselves and others by:

Complying with the Learner Acceptable Use Agreement (LAUA), which is signed as part of the induction process.

Following Academy expectations regarding the use of mobile phones and personal devices, including compliance with the Full Lockdown Procedure and any restrictions on device use during learning activities.

Using Academy systems, devices, internet access and digital resources responsibly and only for authorised educational purposes.

Understanding the importance of reporting any online safety concern, including exposure to inappropriate content, online abuse, cyberbullying, scams, grooming, extremist material, or any behaviour that makes them feel unsafe.

Knowing how and when to report concerns to a trusted member of staff, the Designated Safeguarding Lead/Officer (DSL/DSO), or other appropriate reporting channels.

Understanding that expectations for respectful and safe online behaviour apply both within and outside the Academy where behaviour may impact the safety, wellbeing or reputation of others.

Using Artificial Intelligence (AI) tools and internet search facilities responsibly, ethically and in accordance with Academy guidance, recognising that AI-generated information may be inaccurate, biased or misleading and should always be critically evaluated.

Respecting copyright, intellectual property and academic integrity by producing their own work and appropriately acknowledging the work of others.

Demonstrating respectful online behaviour and treating others with dignity, recognising that online abuse, harassment, discrimination and bullying will not be tolerated.

Use of Artificial Intelligence (AI)

Reflections Training Academy recognises that Generative Artificial Intelligence (GenAI) can enhance teaching, learning and administrative efficiency when used appropriately. The Academy also recognises that AI presents safeguarding, privacy, ethical and academic integrity risks. These risks are managed through existing safeguarding, data protection, cyber security and information governance arrangements, together with ongoing review of emerging technologies.

The Academy will:

support the safe, ethical and responsible use of approved AI technologies;

ensure AI complements, rather than replaces, professional judgement and human decision-making;

ensure staff remain accountable for all work supported by AI;

provide training for staff, governors and learners on the benefits, limitations and risks of AI;

ensure learners develop the skills to critically evaluate AI-generated content;

ensure any AI products used within the Academy meet appropriate safeguarding, security and data protection requirements.

Parents/Carers

- Advice, guidance and information can be found on website
- Signed parental agreement for online sessions and GDPR requirements for learners under the age of 18

Online Safety Education Programme

At Reflections Training Academy/Next Level, we believe that online safety is an integral part of every learner's journey. Developing the knowledge, skills and behaviours needed to navigate the digital world safely is embedded throughout our curriculum and wider skills programme.

Our online safety education is designed to be broad, relevant and progressive, reflecting learners' age, experience and individual needs. The programme is delivered through a range of approaches, including:

Current online safety resources available through the SG/PSHE Padlet.

A monthly wider skills theme that includes online safety where appropriate.

Teaching learners how to evaluate and verify online information before accepting it as accurate, including content generated by Artificial Intelligence (AI).

Developing learners' ability to critically assess the credibility, purpose and potential bias of websites, blogs, social media posts and other online content.

Participation in national initiatives and awareness campaigns, such as Safer Internet Day and Anti-Bullying Week.

Providing accessible learning materials that meet the needs of learners of different ages, abilities and backgrounds, including those with additional learning needs and learners with English as an Additional Language (EAL).

Through our Online Safety Education Programme, learners will develop an understanding of how to:

Follow the Learner Acceptable Use Agreement, which is signed by all learners to promote the safe and responsible use of technology and to protect themselves and others from misuse.

Respond appropriately to inappropriate online content or requests for images, videos or personal information.

Understand the importance of cyber security and adopt good practices to protect devices, accounts and personal data.

Critically evaluate information obtained from a range of online sources.

Maintain a professional and positive digital footprint, including the responsible use of social media.

Apply and regularly review privacy and security settings on online accounts and devices.

Recognise and protect themselves from online scams, fraud, phishing, smishing, quishing, vishing and sextortion.

Use the internet responsibly, including respecting the privacy of others and not sharing images or videos without consent.

Recognise the risks associated with online grooming, exploitation and extremist radicalisation.

Identify the signs and impact of cyberbullying and the sharing of nude or semi-nude images, and know how to seek support.

Report online concerns, abuse or inappropriate behaviour through Reflections Training/Next Level safeguarding procedures, to a trusted adult, or to specialist organisations such as CEOP.

Successfully complete the Prevent it UK Online module and assessment.

Staff Responsibilities

Reflections Training/NEXT Level recognises that promoting online safety is a shared responsibility. Staff are expected to:

Model safe, responsible and professional online behaviour at all times.

Adhere to the Staff Acceptable Use Agreement.

Reinforce online safety messages throughout teaching, learning and learner support.

Respond promptly to online safety concerns in accordance with safeguarding and reporting procedures.

Staff Training and Expectations of Use

Keeping Children Safe in Education (KCSIE) states:

"All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive regular safeguarding and child protection updates (for example, via email, e-bulletins, staff meetings and safeguarding questions of the week), as required, to provide them with relevant skills and knowledge to safeguard children effectively."

At Reflections Training/Next Level, all staff are expected to understand their responsibilities for promoting online safety and safeguarding learners in digital environments. Staff will receive appropriate training to enable them to identify, prevent and respond to online safety concerns in accordance with this policy.

The Academy will ensure that:

A planned programme of online safety, cyber security and data protection training is delivered to all staff. This programme will be regularly reviewed, evaluated and updated to reflect emerging risks, changes in legislation and national guidance.

All staff understand the Four Cs of Online Risk, as identified in KCSIE (Paragraph 163, July 2026):

Content – Exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

Contact – Harmful online interactions with others or generative AI applications that simulate users, including peer pressure, commercial exploitation, inappropriate advertising, and adults posing as children or young people to groom or exploit individuals for sexual, criminal, financial or other purposes.

Conduct – Online behaviours that increase the risk of harm, including cyberbullying, the creation, sharing or receipt of explicit images (including AI-generated images), and other unsafe or inappropriate online behaviour.

Commerce – Risks associated with online financial activity, including gambling, phishing, financial scams, fraudulent activity and inappropriate advertising.

An audit of staff online safety training needs is undertaken at least every two years, with additional training provided where required.

Online safety forms an integral part of the Academy's annual safeguarding, data protection and cyber security training programme.

All new and returning staff receive online safety training as part of their induction programme. This will ensure they understand this policy, associated procedures and acceptable use agreements, and includes guidance on:

safe and effective classroom management when using digital technologies;

maintaining professional boundaries and conduct online;

protecting their professional reputation and digital footprint;

modelling safe, responsible and appropriate online behaviour for learners; and

recognising, responding to and reporting online safety concerns in line with the Academy's safeguarding procedures.

All staff are expected to apply the knowledge gained through training in their day-to-day practice and contribute to a culture where online safety is embedded across teaching, learning and learner support.

Reporting and Responding to Online Safety Incidents

Reflections Training Academy is committed to taking all reasonable steps to safeguard learners, staff and visitors when using digital technologies. While robust preventative measures are in place, the Academy recognises that online safety incidents may occur both within and outside the Academy environment and require an appropriate safeguarding response.

In line with Keeping Children Safe in Education (KCSIE), staff are expected to maintain professional curiosity and immediately raise any concerns about a learner's welfare or online activity with the Designated Safeguarding Lead (DSL), or a Deputy DSL, in accordance with the Academy's safeguarding procedures.

The Academy will ensure that:

Clear reporting procedures are in place, understood by all members of the Academy community and aligned with safeguarding, whistleblowing, complaints and managing allegations procedures.

All staff and learners understand their responsibility to report online safety concerns, incidents or suspected misuse of digital technologies.

All reports are treated seriously and responded to as quickly as reasonably practicable.

The Designated Safeguarding Lead (DSL) and other appropriate staff receive regular training to enable them to manage online safety concerns effectively and confidently.

Individuals reporting an online safety concern are supported throughout the process and have confidence that concerns will be handled fairly, sensitively and confidentially.

Incidents Requiring Immediate Safeguarding Escalation

Where there is any suspicion of illegal activity or a risk of significant harm, the incident must be managed through the Academy's safeguarding procedures and, where appropriate, referred to external agencies, including the Police, Children's Social Care, the Local Authority Designated Officer (LADO), CEOP or other relevant organisations.

Examples include, but are not limited to:

Non-consensual sharing of intimate images.

Self-generated or self-shared explicit images involving children or young people.

Child Sexual Abuse Material (CSAM).

Child sexual exploitation or online grooming.

Terrorism, extremist content or radicalisation.

Hate crime or online abuse.

Harassment, stalking or malicious communications.

Fraud, extortion, phishing or sextortion.

Cybercrime or hacking offences under the Computer Misuse Act.

The sale or promotion of illegal goods or substances.

Extreme pornography.

Copyright infringement or digital piracy.

Concerns Involving Staff

Any concern regarding the misuse of technology by a member of staff will be reported immediately to the Directors. Where the allegation concerns a Director, the matter will be referred to the Chair of Governors and the Local Authority Designated Officer (LADO) in accordance with the Academy's Managing Allegations Policy.

Investigation of Devices

Where there is no immediate suspicion of illegal activity, devices may be examined as part of an internal investigation. Any examination will:

Be authorised and undertaken by one or more senior members of staff to ensure fairness, transparency and accountability.

Be conducted in accordance with the Academy's safeguarding, data protection and acceptable use procedures.

Be fully documented, including the reasons for the examination and those involved.

Cease immediately if evidence suggests illegal activity, at which point the device will be secured and referred to the Police or other appropriate authority. Staff will not continue investigating potential criminal matters.

Be repeated separately for any additional devices identified during the investigation.

Where online content forms part of the investigation, authorised staff may record relevant website addresses (URLs), descriptions of the content and, where appropriate and lawful, secure screenshots or other evidence. All evidence will be stored securely, handled in accordance with data protection legislation and retained in line with the Academy's retention schedule.

Artificial Intelligence (AI) tools must not be used to monitor individuals, investigate incidents or generate safeguarding records or incident reports.

Outcomes and Follow-up

Following the investigation, the Academy will determine whether the concern is substantiated and take appropriate action. This may include:

Internal support, education or disciplinary action.

Referral to safeguarding partners or the Local Authority.

Referral to external agencies, including the Police, where appropriate.

Review of risk assessments and safeguarding arrangements.

Additional support for those affected by the incident.

Those directly involved will receive appropriate feedback on the outcome, where this is lawful and appropriate to share.

Recording and Learning from Incidents

All online safety incidents and concerns will be:

Recorded on the Academy's Online Safety Reporting Log.

Stored securely within the Academy's protected OneDrive safeguarding records.

Monitored to identify patterns, emerging risks and areas for improvement.

Learning arising from incidents will be used to strengthen practice and, where appropriate, shared anonymously through:

Safeguarding Group meetings to review policies, procedures and education programmes.

Staff briefings and safeguarding updates.

Learner wider skills and online safety sessions.

Communications with parents, carers and stakeholders, where appropriate.

Reports to Governors.

Information sharing with the Local Authority, LADO and other external agencies where required.

The Academy will provide staff with an Online Safety Incident Response Flowchart to support consistent decision-making and ensure concerns are managed promptly, proportionately and in accordance with safeguarding and statutory guidance.

Academy Actions

Reflections Training/Next Level recognises that the majority of online safety concerns are likely to involve inappropriate rather than illegal use of technology. It is essential that all incidents are responded to promptly, proportionately and consistently, ensuring that those involved receive appropriate support while maintaining a safe and respectful learning environment.

Where appropriate, incidents of inappropriate online behaviour will be managed through the Academy's Behaviour Policy, Complaints Policy, Acceptable Use Agreements and safeguarding procedures. Members of the Academy community will be made aware that concerns are taken seriously and addressed appropriately, while maintaining confidentiality for those involved.

Cyber Security

The Academy recognises that cyber security is a leadership, governance and safeguarding responsibility. In line with Keeping Children Safe in Education (KCSIE) 2026) and the Department for Education (DfE) Cyber Security Standards, the Academy takes proactive steps to reduce both the likelihood and impact of cyber security incidents.

The Academy will ensure that:

A robust cyber security approach is in place to prevent, detect, respond to and recover from cyber threats.

Directors and senior leaders understand cyber security risks and receive appropriate assurance regarding the effectiveness of cyber security arrangements.

Staff and learners receive appropriate education and training to recognise, prevent and report cyber security concerns.

Business continuity, disaster recovery and cyber incident response plans are maintained, tested and reviewed regularly.

Cyber security controls and procedures are reviewed periodically to reflect emerging technologies, threats and national guidance.

Data Protection and Information Governance

The Academy is committed to protecting personal information and complying with all applicable data protection legislation, including the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

The Academy will ensure that:

Personal data is processed lawfully, fairly and transparently.

A designated Data Protection Officer (DPO) is appointed and effective governance arrangements are maintained.

All staff receive regular data protection training and understand their responsibilities for handling personal information securely and reporting data breaches.

Appropriate procedures are in place to manage Subject Access Requests (SARs) and Freedom of Information (FOI) requests.

Data Protection Impact Assessments (DPIAs) are completed where required before introducing new systems, software or technologies.

Privacy notices clearly explain how personal information is collected, used, stored, shared and individuals' rights can be exercised.

Personal information is stored, shared, retained and disposed of securely in accordance with the Academy's Data Protection Policy and Records Retention Schedule.

Data breaches are reported, investigated and managed in accordance with legal and regulatory requirements.

Data protection principles are embedded throughout safeguarding, teaching, learning and business operations.

Where Artificial Intelligence (AI) or automated decision-making technologies are used, appropriate human oversight will always be maintained for significant decisions. Risk assessments will be undertaken, and AI systems will be transparent, explainable and used in accordance with Academy policy and legal requirements.

Mobile Phones and Smart Devices

In line with the Academy's Behaviour Policy, Learner Acceptable Use Agreement and current Department for Education guidance, learners are expected to use mobile phones and smart devices responsibly whilst on Academy premises or participating in Academy activities.

The Academy may restrict or prohibit the use of mobile phones and other internet-enabled smart devices during learning sessions or other designated times where their use could disrupt learning, compromise safeguarding or present an online safety risk.

AI-Generated and Self-Generated Images and Videos

The Academy recognises the increasing risks associated with the creation, sharing and manipulation of digital images and videos, including content generated using Artificial Intelligence (AI).

This includes, but is not limited to:

Self-generated or self-shared intimate images or videos.

Non-consensual sharing of intimate images.

AI-generated or manipulated images, including deepfakes.

Unauthorised or inappropriate photography or video recordings.

Content that promotes or encourages self-harm, suicide, eating disorders, violence, extremism or other harmful or illegal activity.

Any online material that is illegal, abusive or requires reporting to safeguarding or law enforcement agencies.

Any learner or member of staff who becomes aware of such content must report their concerns immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL.

Investigation and Recording

All online safety incidents, concerns or allegations will be:

Recorded using the Academy's Online Safety Incident Reporting Form.

Reviewed by the Designated Safeguarding Lead (DSL) and, where appropriate, the Academy Directors.

Risk assessed to determine the appropriate safeguarding, disciplinary or legal response.

Managed in accordance with the Academy's safeguarding, behaviour, data protection and disciplinary procedures.

Referred to external agencies, including the Police, Local Authority Designated Officer (LADO), Children's Social Care or CEOP, where appropriate.

The Academy is committed to learning from online safety incidents. Outcomes and emerging themes will be used to inform staff training, learner education, policy reviews and continuous improvement of online safety practice across the organisation.