Online Safety and Social Media Policy

Version Control: 1.0
Effective From Date: February 2026
Responsible Officer: Head of Quality and Safeguarding
Approved by: Governors / CEO
Review Due: 16/02/2027

Summary of Changes

Version	Review date	Comments
1.0	16/02/26	A full review of the policy; revised to reflect current statutory requirements, including Keeping Children Safe in Education (KCSIE) 2025, cross-referenced and aligned with related internal policies, including Safeguarding & Child Protection, Behaviour, Acceptable Use, Data Protection and Staff Code of Conduct. This policy replaces the previous E-Safety Policy, Mobile Phone Policy and AI Policy, bringing all digital safeguarding and technology-related expectations into one coherent framework.

Contents

1. Purpose

New technologies have become integral to the lives of Runway Training staff, learners and apprentices, both in their work and learning environments and in their lives outside work and learning. The internet and other digital and information technologies are powerful tools that create new opportunities for everyone.

Electronic communication helps staff, learners and apprentices learn from one another. These technologies can stimulate discussion, promote creativity and increase awareness of context, thereby supporting effective learning. Learners and apprentices have an entitlement to safe internet access.

Runway Training recognises the growing role of generative artificial intelligence (AI) in learning and the potential risks and opportunities it poses. In line with Keeping Children Safe in Education and the Department for Education's guidance on AI use in schools and colleges, we are committed to ensuring that any use of generative AI within Runway Training upholds the safeguarding, privacy, and well-being of all learners, apprentices, and staff.

Runway Training aims to:

- Safeguard and protect all members of the Runway Training community online.
- Identify approaches to educate and raise awareness of online safety, e-safety, social media safety and mobile technology safe usage throughout the community.
- Enable all staff to work safely and responsibly, to role model positive online behaviour, and to manage professional standards and practice when using technology.
- Identify clear procedures for responding to online safety concerns.

Runway Training identifies that the issues classified under online safety are considerable but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material.
- Contact: being subjected to harmful online interaction with other users.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce: identify risks of inappropriate behaviours such as gambling, phishing or financial scams. Balance opportunities without over-blocking. Use of AI tools will be subject to risk assessments led by the Head of Quality and Safeguarding or DSL in their absence. AI will not be used to make decisions affecting an individual, for example, safeguarding or attendance, and will comply with GDPR and related Data and Information Security/IT Policies.

Many of these risks mirror offline scenarios, and it is essential that this policy be used alongside other linked Runway Training policies. As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through effective educational provision, to build learners', apprentices' and staff's resilience to the risks they may be exposed to, so they have the confidence and skills to address them.

2. Scope

This policy applies to all members of Runway Training, including staff, learners, apprentices, governors, and visitors. It also applies to individuals who use our services or are employed by agencies, contractors, or subcontractors.

- Staff, learners, and apprentices working or studying on premises not owned by Runway Training will continue to be subject to the policy.
- Any breaches of this policy will be treated seriously and may result in disciplinary action.

This policy has been agreed upon, sponsored by the Chief Executive Officer, and authorised by the Governors.

3. Policy Statement

This policy outlines how Runway Training fulfils its statutory duties and other requirements relating to online safety, e-safety, and social media use, including the use of photographs and mobile phones. It sets out expectations for all staff, learners, apprentices, and other stakeholders regarding online and e-safety and social media use, covering governance, oversight, safeguarding practice, education and conduct on and off our premises, as well as when using Runway Training-owned and privately owned equipment.

The policy covers the use of all online media, including, but not restricted to:

- The internet
- Mobile phones
- Systems designed to support learning, used in Runway Training, such as Microsoft Teams
- Social media
- Text messages and messaging apps
- Email
- Virtual Learning Environments
- AI (Artificial Intelligence)
- Blogs
- Podcasting
- Music Download sites
- Online chats
- Online gaming and gambling sites
- Digital cameras
- Live streaming sites.

There are several areas of abuse and concern that our approach and policy seek to address.

The list below is not exhaustive but includes:

- Online bullying and harassment
- Relationship abuse
- Sharing of nudes and semi-nudes
- Cyber Crime (as both potential victim and perpetrator)
- Emotional abuse
- Grooming (including into exploitation and radicalisation)
- Access to inappropriate content, including pornography
- Risk-taking behaviour such as online gambling
- Online reputation and digital footprint

4. Definitions

Online Safety: The practice of safeguarding users of digital technology, including the internet and electronic communication devices, from harm such as cyberbullying, inappropriate content, and online predators.

Filtering Systems: Technology that blocks access to inappropriate or harmful online content while allowing access to necessary and educational material.

Monitoring Systems: Tools and processes used to track and review the use of digital devices and internet access to ensure compliance with online safety policies.

Acceptable Use: A set of rules and guidelines that outline the appropriate use of Runway Training's IT systems and internet access, which all users must agree to and follow.

Cyberbullying: Bullying that occurs online or through digital communication, often involving repeated, intentional harm to an individual or group via social media, messaging apps, or gaming platforms.

Digital Technology: Electronic tools, systems, devices, or resources that generate, store, or process data, including computers, smartphones, tablets, the internet, and social media platforms.

Safeguarding: The practice and actions of protecting children, young people and vulnerable adults from abuse, harm, and neglect, thereby ensuring their well-being and safety.

Adults At-Risk (Vulnerable Adults): Individuals aged 18 or over who are at increased risk of harm or exploitation due to factors such as age, disability, illness, or personal circumstances.

Radicalisation: The process by which an individual or group adopts increasingly extreme political, social, or religious ideals and aspirations, potentially leading to terrorism.

GDPR UK (General Data Protection Regulation): A regulation that sets guidelines for the collection and processing of personal information from individuals in the United Kingdom (UK), ensuring data privacy and protection.

Nudes/semi-nudes: The act of sending or receiving sexually explicit messages or images, typically between mobile devices.

Addiction: Addiction is most commonly associated with drugs, gambling and alcohol, but it can also describe a broad range of online behaviours, such as online gaming addiction (internet gaming disorder), online gambling addiction, social media addiction, mobile phone addiction, or even internet addiction in general.

Artificial Intelligence-Generated Abuse: Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, particularly computer systems. AI is being used to generate indecent images of children. Child sexual abuse images are illegal in the UK, regardless of how they are produced.

Chatbots: A chatbot is a software application that simulates human-like conversation through text or voice interactions. Children using chatbots face potential risks, including exposure to inappropriate content, privacy breaches due to data collection, and vulnerability to cyberbullying and misinformation.

Cyberflashing: Cyberflashing is the act of sending sexual images or pornography to an unsuspecting person digitally. Because the images are sent via channels other than the app, the victim will not know they have been cyberflashed until they open the notification or open the app.

Deepfake: A deepfake is an image, video, sound, voice, or GIF that has been manipulated by a computer to superimpose someone's face, body, or voice onto another person or object. This can be done with or without the subject's consent.

Extremism: Defined as 'the vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs,' it refers to an ideology considered outside the mainstream attitudes of society. Radicalisation is the process by which someone changes their perceptions and beliefs to become more extremist. Extremists use the online space to target and exploit vulnerable people and to spread divisive propaganda and disinformation.

Gaming and Livestreaming: Livestreaming is the practice of broadcasting oneself or others to an online audience in real time. Many social media platforms offer livestreaming features that are open to anyone but are often used by gamers, celebrities, or influencers to communicate with a targeted audience. It has also been used by criminals to livestream their activities and by those perpetrating abuse against a victim.

Identity Theft: When your personal details are stolen. Criminals are increasingly using technology in more complex ways, often employing social engineering tactics such as fear or urgency to lure people into revealing personal information, for example, through phishing scams.

Misinformation: Misinformation, or 'fake news', is online content that can mislead or provide false information on a particular topic. Stories are often fabricated to create panic or concern, and they rely heavily on users to critically assess what is trustworthy. Staff should educate learners and apprentices on how to 'fact-check' information.

Online Challenges: Online challenges or hoaxes often appear on social media and other platforms. The 'challenges' themselves can vary, but they often encourage individuals to harm themselves, others, or property in the real world. They are often designed to alarm and to appear enticing or exciting to young people.

Online Sexual Harassment: Online Sexual Harassment is unwanted sexual contact on a digital device that negatively impacts another person. This can take many forms, both online and offline, such as unwanted sexualised messages, sharing unsolicited intimate imagery, requesting sexualised messages or imagery, doctoring or editing imagery to make people appear to be in intimate or sexualised situations, sexualised insults or name-calling, and leaving sexually suggestive comments on someone's online content. The Online Safety Act makes this activity illegal and may result in a fine, a criminal record, and imprisonment for the perpetrator.

5. Responsibilities

Governors are responsible for:

- Governors are responsible for approving the online safety policy and for reviewing its effectiveness.
- All governors will ensure they have read and understand this policy.
- Do all that is reasonably possible to limit learners' and apprentices' exposure to risks arising from Runway Training's IT system.
- Ensure Runway Training has appropriate filtering and monitoring systems in place and review their effectiveness.
- Ensure that the senior leadership team and relevant staff are aware of the provisions in place, manage them effectively, and know how to escalate concerns.
- Consider the number and age range of their learners and apprentices, those who are potentially at greater risk of harm, how often they access the IT system, and the proportionality of costs versus safeguarding risks.
- Ensure online safety training for all staff as part of safeguarding training.
- Review the policy and associated procedures annually.
- Implement and monitor the consistent application of this policy.
- Agree to and adhere to the terms on acceptable use of Runway Training's IT systems and the internet.
- Ensure that online safety education is adapted for vulnerable children and young people, victims of abuse, and those with special educational needs and/or disabilities (SEND) where necessary, recognising that a 'one size fits all' approach may not be suitable.

The Head of Quality and Safeguarding and the Safeguarding Team are responsible for:

- The Head of Quality and Safeguarding will lead on online safety within Runway Training.
- Ensure incidents are logged, reviewed and reported appropriately.
- Provide training and updates to staff, learners and apprentices on online safety.
- Ensures that the Online Safety Policy is effectively implemented across the organisation, supporting the CEO and other staff.

- Reviews the Online Safety Policy with the safeguarding team and governors, ensuring updates are incorporated as necessary.
- Takes the lead in understanding and managing the filtering and monitoring systems on Runway Training's devices and networks.
- Works closely with the external IT support organisation and other relevant staff to promptly address online safety issues or incidents.
- Ensures that incidents of cyber-bullying are logged and managed in line with the Behaviour and Disciplinary Policy.
- Conducts self-audits as needed to assess training needs.
- Coordinates with external agencies and services when necessary to support online safety.
- Provides regular reports on online safety issues to the SLT and the governors.
- Conducts annual risk assessments to identify and address the risks learners and apprentices face online.
- Ensures the Online Safety Policy and updates are accessible to all staff via SharePoint and the website.
- Take lead responsibility for online safety within their safeguarding role, ensuring they receive relevant and regularly updated training to enable them to understand the risks associated with online safety, be aware of the potential for serious child protection concerns and have the relevant knowledge to keep individuals safe while they are online.
- The Head of Quality and Safeguarding will meet monthly with the Safeguarding Governor to discuss current issues, review incidents and filtering and monitoring logs, and ensure that annual filtering and monitoring checks are carried out. Reporting monthly to the SLT at SLT meetings and to Governors at Governor meetings on the organisation's response to safeguarding and online safety.
- Work collaboratively to promote online safety education, raising awareness across the organisation through staff training, curriculum design, and engagement with national initiatives.
- Ensure staff are aware of the procedures to follow in the event of an online safety incident and of adherence to the Safeguarding – Reporting a Concern Procedure. The Head of Quality and Safeguarding will consult with the CEO and technical staff on matters related to digital safety, cybersecurity and filtering and monitoring systems. This will include reviewing the Online Safety Policy and processes, as well as incident logs, to inform online safety developments.
- The Safeguarding Team is responsible for the day-to-day management of online safety incidents that raise a child protection or safeguarding concern, in line with Runway Training's Safeguarding and Child Protection Policy and the Safeguarding – Reporting a Concern Procedure.
- The Head of Quality and Safeguarding will act as a single point of contact (SPOC) for all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up to date with current research, legislation and trends on online safety, and communicate these with the community, as appropriate.
- Ensure that online safety is promoted among parents, carers and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns and actions taken as part of Runway Training's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use the findings to update the education response, policies and procedures.
- Ensures that all staff receive annual refresher/update training on online safety, which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Ensures all staff understand the differences between filtering and monitoring, and who is responsible for filtering and monitoring
- Liaises with the Local Authority and Police, as necessary.

Management is responsible for:

The CEO is responsible for overseeing the implementation of the arrangements set out in this policy.

- Implements and regularly reviews security measures, including filtering and monitoring systems, to safeguard individuals from harmful online content.
- Regularly monitors Runway Training's IT systems, reporting any misuse to the Head of Quality and Safeguarding.
- Ensures all online safety incidents are logged and addressed according to the Behaviour or Disciplinary Policy.
- Reports any incidents of cyber-bullying to the appropriate manager, ensuring they are handled according to policy.
- Maintains the technical infrastructure to prevent misuse or malicious attacks, ensuring that all users have secure usernames and passwords.
- Keeps an up-to-date record of users and their access credentials, requiring users to change their passwords every six months.
- Regularly monitors the filtering and monitoring reports, following procedures as required. Escalating concerns for staff as appropriate.
- Ensures that online safety is embedded within a progressive curriculum, which enables all learners and apprentices to develop an age-appropriate understanding of online safety.
- Supports the Head of Quality and Safeguarding and the Safeguarding Team by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practices to identify strengths and areas for improvement.

IT Provider is responsible for:

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both Safeguarding and IT staff to be effective. Our IT service provider has technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports and completing actions following concerns or checks of systems
- The IT Provider is responsible for ensuring Runway Training's technical infrastructure is secure and not open to misuse or malicious attack, and ensuring any misuse is identified and reported to the CEO and Head of Quality and Safeguarding for investigation and action.
- Provide technical support and perspective to the Head of Quality and Safeguarding and SLT, especially in the development and implementation of appropriate online safety practices.
- Implement appropriate security measures as directed by the Head of Quality and Safeguarding and SLT (such as password policies and encryption) to ensure that the organisation's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- That Runway Training meets the online safety technical requirements outlined in the GDPR, Data Protection, and Data and Information Security Management Policy.
- That users may only access our networks through properly enforced password protection, in which passwords are regularly changed
- That processes are applied and updated on a regular basis.
- That the use of the network/Virtual Learning Environments (VLEs) is regularly monitored in order that any misuse/attempted misuse can be reported

The IT Provider will work with the Head of Quality and Safeguarding to:

- Review the filtering and monitoring provision at least annually.
- Conduct regular checks on the filtering and monitoring systems, at least once per quarter.
- Ensure the Head of Quality and Safeguarding (and/or DSL) have appropriate access to and technical support for our filtering and monitoring systems, enabling them to take appropriate safeguarding action if and when required.
- Maintain awareness of technical developments that may affect Runway Training's online policies and procedures, and work with the Head of Quality and Safeguarding to make adjustments as required.
- The IT Provider will implement and maintain secure IT systems, including filtering and monitoring.

Staff are responsible for:

- All staff must understand and consistently apply the Online Safety Policy.
- Ensure compliance with the terms of Runway Training for IT systems and the internet and guide learners and apprentices to comply as well.
- Report any incidents involving filtering and monitoring systems to the DSL for appropriate action.
- Assist learners and apprentices in understanding appropriate online behaviour and in reporting any concerns about misuse or inappropriate content.
- Tailor educational support for vulnerable children, young people and adults, including those with SEND, and seek advice as required.
- Manage any incidents of cyber-bullying in accordance with the Behaviour or Disciplinary Policy, ensuring a prompt and appropriate response.
- Remain vigilant during sessions and visits, particularly when learners and apprentices are conducting independent research, and report any misuse to IT services or the safeguarding team.
- Engages with staff, parents, and carers to gather feedback and improve online safety measures.
- Monitors the implementation of actions identified through self-review tools, ensuring continuous improvement.
- Always act in the best interests of learners and apprentices.
- Act in accordance with professional boundaries, upholding professional behaviour and conduct at all times.
- Be aware of and adhere to all policies in Runway Training that support online safety and safeguarding.
- Support in taking responsibility for the security of systems and the data accessed.
- Model good practice when using technology and managing mobile phone use in sessions, whilst being able to use them for educational purposes where appropriate.
- Play a key role in monitoring learners' and apprentices' use of technology in Runway Training. This includes direct supervision in the training room and, in line with usual safeguarding practice, being alert to their safety in other contexts. It also includes challenging inappropriate use when witnessed and reporting concerns.
- Know and follow the process for making referrals and reporting safeguarding concerns.
- Know how to recognise, respond to and report signs of online abuse and harm.
- Engage in mandatory safeguarding and Prevent training.
- Be responsible for their own continuing professional development in online safety.
- All staff understand that online safety is a core part of safeguarding and have read and understood the relevant Runway Training Policies.
- All staff must ensure that digital communications with learners, apprentices and parents/carers are professional and carried out only using Runway Training systems.
- All staff should model safe, responsible, and professional online behaviour in their own use of technology and maintain a professional standard of conduct in their personal use of technology, both on and off-site.

- All staff working with learners and apprentices should ensure that learners and apprentices understand and follow the relevant IT Policies, comply with the Disciplinary Policy and codes of conduct, and maintain a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination, extremism, etc.
- In sessions where internet use is pre-planned, learners should be guided by staff to sites deemed suitable for their use, and processes should be in place to address any unsuitable material found during internet searches. Any inappropriate or harmful content should be reported to the Head of Quality and Safeguarding to ensure it can be blocked by filtering systems. As per our Safeguarding Policy and Safeguarding – Reporting a Concern Procedure, all staff should act immediately to prevent harm to learners and apprentices online or inform the Safeguarding Team if they believe a learner or apprentice is at risk of harm – online or offline. In sessions conducted via live streaming or videoconferencing, staff must comply with guidance on the safe use of remote learning resources.
- Contribute to the development of online safety policies.
- Take responsibility for the security of the systems and data used or accessed.
- Embed online safety education in curriculum delivery, wherever possible
- Know when and how to escalate online safety issues, including signposting to appropriate internal and external support.
- Take personal responsibility for professional development in this area.

Learners and Apprentices are responsible for:

- Adhering to this policy.
- Reporting any online safety concerns or incidents to the DSL.
- Be aware that whilst they are permitted to bring their mobile phones or other smart devices to Runway Training, they should use them only as necessary and with respect for other learners, apprentices and the teacher or employment adviser during the session. Be aware of how to access the Safeguarding Team, report concerns and seek help when needed.
- Engage with the online safety education provided, following the behaviours outlined by the teacher or employment adviser.
- Behave respectfully towards others online, including in their use of mobile phones.
- Take responsibility for keeping themselves and others safe online.
- Learners should understand the importance of reporting abuse, misuse, or access to inappropriate or harmful materials, know how to do so, and know what to do if they or someone they know feels vulnerable when using online technology.
- Learners should understand the importance of adopting good online safety practices when using digital technologies outside Runway Training and realise that the Online Safety Policy applies to their actions outside our learning and work environments, provided they are related to their programme of learning with Runway Training.
- Are responsible for Runway Training's IT systems in accordance with the Acceptable Use of Computers Agreement, which they will be expected to 'accept' as part of their induction process.
- Have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations

All new employees are made aware of this policy and procedures during the formal employee induction process. All learners and apprentices are made aware during their induction, in their handbooks, and during training and learning with Runway Training. Updated and amended procedures are discussed in training sessions, team meetings, and via email communications, as appropriate. This policy is available to all staff, learners, apprentices, and other stakeholders via the relevant systems.

Runway Training will be responsible for ensuring that the infrastructure and network are as safe and secure as reasonably possible and that policies and procedures are implemented and embedded. It will also ensure that the relevant people named in this policy are effective in fulfilling their responsibilities.

- IT systems will be managed to ensure Runway Training meets technical requirements
- Regular reviews and audits will be conducted of the safety and security of IT systems
- IT systems and equipment will be appropriately secured in line with relevant IT, Data and Information Security Policies
- All users will have clearly defined access rights to Runway Training's IT systems. Details of the access rights available to user groups will be recorded by the External IT outsourcing company and the Head of Quality and Safeguarding.
- All users will be provided with a username and a password
- Users will be responsible for the security of their username and password. They must not allow other users to access the systems using their login credentials and must immediately report any suspicion or evidence of a security breach.
- Where necessary, monitoring is carried out in line with Runway Training's policy
- IT technical staff may monitor and record the activity of users on the IT systems, and users are made aware of this in the GDPR, Data Protection, and Data and Information Security Policy
- An appropriate system is in place for users to report any actual or potential incidents in line with the above policy and the Safeguarding Policy.
- Guidelines are in place regarding the extent of personal use permitted on laptops and other portable devices that may be used outside Runway Training
- Guidelines are in place to control what software staff can install on Runway Training's workstations and portable devices
- Runway Training's infrastructure and individual workstations are protected by up-to-date antivirus software.
- Personal data should not be sent over the internet or removed from Runway Training's premises unless it is securely encrypted or otherwise protected

6. Curriculum Focus

Online and e-safety should be a focus across the curriculum, and employees should reinforce these messages in IT use and through activities.

- In sessions where internet use is pre-planned, it is best practice to guide learners and apprentices to sites that have been checked for suitability, and to have processes in place to deal with any unsuitable material found during internet searches.
- Where learners and apprentices are allowed to freely search the internet, e.g. using search engines, employees should be vigilant (as far as possible) in monitoring the content of the websites they visit.
- It is accepted that, from time to time, for good educational reasons, learners and apprentices may need to research topics (e.g. racism, drugs, and discrimination) that would normally be blocked by internet filters. In such a situation, employees may request that the external IT company temporarily remove those sites from the filtered list for the duration of the learning. Any such request should be auditable and supported by clear reasons for the need. Such requests must be made via the DSL.
- Learners and apprentices should be taught to acknowledge the source of information and to respect copyright when using material found online.

7. Use of Digital and Video Images - Photographic, Video

The development of digital imaging technologies has brought significant benefits to learning, allowing employees, learners and apprentices to use images they have recorded themselves or downloaded from the internet. However, individuals should be aware of the risks of sharing images online. Those images may remain online indefinitely and could cause harm or embarrassment to individuals in the short or long term. There are many reported incidents of employers conducting online searches about potential and current employees. Runway Training will inform and educate users about these risks and implement policies to reduce the likelihood of harm.

When using digital images, employees should inform and educate learners and apprentices about the risks of taking, using, sharing, publishing and distributing images. In particular, they should recognise the risks of publishing their own images online, for example, on social networking sites. Employees are permitted to take digital or video images to support educational aims, but must follow Runway Training policies on the sharing, distribution and publication of those images. Those images should be taken only on Runway Training equipment. Employees' personal equipment should not be used for such purposes.

Care should be taken when taking digital or video images to ensure that learners and apprentices are appropriately dressed and not participating in activities that might bring them or Runway Training into disrepute.

8. GDPR

- Learners and apprentices must not take, use, share, publish or distribute images of others without their permission and should seek clarification from a Runway Training member of staff if they are unsure
- Photographs published on the website or elsewhere that feature learners, apprentices and staff will be selected carefully and will comply with good practice guidance on the use of such images.
- Staff, learners and apprentices' full names will be used only where their or their parents'/guardians' written consent has been sought (where necessary) for use on a website or blog, particularly in association with photographs
- Where necessary, written permission from parents or guardians will be obtained before photographs of younger or at-risk learners and apprentices are published on Runway Training's website.
- Learners' and apprentices' work can be published only with the individual's permission and, where necessary, the parents' or guardians' permission
- Where any staff member, learner or apprentice is a Child in Care or a Care-Experienced Leaver, express written permission must be obtained before publishing any information, in particular photographs, of the individual to ensure their safety.

9. Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with the General Data Protection Regulation (GDPR UK) 2018, the Data Protection Act 2018, and the UK's Data Use and Access Act June 2025, which state that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

Personal data will be transferred to relevant parties only if adequate protection measures are in place. Following a number of "high-profile" personal data breaches by public organisations, training providers are likely to face greater scrutiny of their personal data handling. Please also refer to the GDPR and Data Protection, and the Data and Information Security Policy for further information.

10. Communications

A wide range of rapidly developing mobile communications technologies has the potential to enhance learning.

When using mobile communication technologies, Runway Training considers the following good practice:

- Employees, learners and apprentices should therefore use the Runway Training email service only to communicate with others when at Runway Training or on Runway Training systems (e.g. via remote access)
- Users need to be aware that email communications may be monitored
- Users must immediately report to their line manager/teacher or employment adviser the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying, and must not respond to any such email
- Any digital communication between employees and learners, apprentices or parents/guardians (email, chat, VLE, etc.) must be professional in tone and content. These communications may only take place on official Runway Training systems that comply with the Acceptable User/Usage section of the GDPR and the Data Protection and Data and Information Security Policy.
- Personal email addresses, text messaging, or public chat or social networking programmes must not be used for these communications. The exception applies to LinkedIn.com for career development activities.
- Learners and apprentices should be taught about email safety, including the risks of sharing personal details. They should also be taught strategies for handling inappropriate emails and reminded to write emails clearly and correctly, without including any unsuitable or abusive material.
- Personal information should not be posted on Runway Training's website, and only official email addresses should be used to identify employees.
- Personal mobile telephone numbers must not be disclosed to learners and apprentices

11. Unsuitable / Inappropriate Activities

Some internet activities, e.g. accessing child abuse images or distributing racist material, are illegal and are banned from all Runway Training's IT systems. Other activities, e.g., cyberbullying, are banned and could lead to criminal prosecution.

12. Responding to Incidents of Misuse

It is hoped that all members of the Runway Training community will be responsible users of digital technologies and understand and follow this policy, its procedures, and its guidelines. However, there may be times when policy infringements occur through carelessness or irresponsibility, or, very rarely, through deliberate misuse.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- If any apparent or actual misuse appears to involve illegal activity, i.e., child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

If a safeguarding issue is disclosed, the Safeguarding Policy should be consulted, and actions should be taken in line with the flowchart, particularly the sections on reporting the incident to the police and on preserving evidence.

If employees suspect misuse that is not illegal, it is essential to follow the correct procedures to investigate, preserve evidence, and protect the investigators. If anyone suspects that an individual is accessing an illegal website, the website should not be accessed by the individual but reported in line with Runway Training's Safeguarding Policy. It is more likely that Runway Training will need to deal with incidents involving inappropriate rather than illegal misuse.

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Runway Training community are informed that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through Runway Training's behaviour/disciplinary procedures.

13. Web Filtering

- Runway Training maintains and supports the managed web filtering service.
- If the external IT support organisation needs to disable filtering for any reason or for any user, this must be logged and carried out through a process agreed by the Head of Quality and Safeguarding or, in their absence, the Chief Executive Officer.
- Requests from employees for sites to be removed from the filtered list will be considered by the Head of Quality and Safeguarding and the external IT support organisation.

14. Computer Network Acceptable User – Staff

General Principles

Use of Runway Training's network systems and services, including but not limited to the Internet, intranet, email and SMS, will be monitored for unusual activity and for security and/or network management purposes. Users may also be subject to limitations on their use of these resources.

Correspondence via email or other electronic means cannot be guaranteed to be private. Any confidential email should be sent only using encryption techniques approved by Runway Training.

The distribution of any information via the Internet, computer-based services, email and messaging systems is subject to scrutiny. Runway Training reserves the right to determine the suitability of this information. Limited personal use of the Internet and email services is permitted for skills development, but is subject to the terms set out below.

15. Conditions of Use

Users must not:

Visit Internet sites that contain obscene, hateful or other objectionable materials; send or receive by electronic means material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person.

This includes, but is limited to, the following:

- Child sexual abuse images
- Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of self-harm or suicide
- Any other information that may be offensive to colleagues, breach the integrity of the ethos of the Runway Training, or bring Runway Training into disrepute
- Solicit non-Runway Training business for personal gain or profit
- Use the Internet, email, telephone system or SMS service for any illegal purpose

- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards used by Runway Training
- Represent opinions as those of Runway Training
- Make or post indecent remarks, proposals or materials
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside Runway Training or to Runway Training itself
- Install or run any unauthorised software on Runway Training equipment. Download any software or electronic files without implementing virus protection measures approved by the Runway Training.
- Intentionally interfere with the normal operation of the network, including, but not limited to, the propagation of computer viruses and sustained high-volume network traffic that substantially hinders other users' use of the network
- Use Internet, email or SMS services for inappropriate personal use not connected with Runway Training business
- Reveal or publicise confidential or proprietary information, including, but not limited to financial information, new business ideas, marketing strategies and plans, databases and the information they contain, learner and apprentice enrolment details, and business relationships
- Transfer or upload personal data, as defined by the GDPR Data Protection Act, to any device, equipment or system not owned by Runway Training without the express permission of the Head of Quality and Safeguarding and the external IT support organisation
- Transfer personal data, as defined by the GDPR Data Protection Act, to any portable storage device, e.g. a USB stick, even if the device is owned by Runway Training, without the express permission of the Head of Quality and Safeguarding and the external IT support organisation
- Examine, change or use another user's files, output or username for which they do not have explicit authorisation
- Reveal individual passwords, whether account logon or system-specific, to anyone else
- Resell any service provided by Runway Training, including, but not limited to, email, network storage and Internet access
- Perform any other inappropriate uses identified by the Head of Quality and Safeguarding and the external IT support organisation
- Users who violate any of the procedures or guidelines set out in the policy may be subject to disciplinary action and/or legal action, which may result in a criminal conviction. Runway Training also retains the right to report any illegal activities to the appropriate authorities.

16. Monitoring and Reporting

- Staff training records
- The design and content of the curriculum
- Assessment of learners' and apprentices' understanding
- Feedback received from learners, apprentices and staff
- Self-Assessment Report and Quality Improvement Plan activities and review
- Board Reports from each team
- Comments, compliments and complaints received from learners, apprentices and other stakeholders
- Safeguarding reports, including Filtering and Monitoring reporting
- Quality reports
- Learner, apprentice and staff surveys
- Disciplinary and behaviour records
- The SLT, Board and Governors' meeting minutes and actions
- Recruitment and induction of staff, learners and apprentices
- Feedback received from learners, apprentices, employers and staff and any improvements or alterations to the procedures
- The volume of concerns/disclosures raised, and actions taken

17. Effectiveness will be measured through:

- Learners and apprentices completing their programme of learning and not leaving the programme early due to online/e-safety and related topics, safeguarding concerns that have not been recognised or addressed
- Observations of staff to ensure they are embedding online/e-safety, safe use of mobile phone and social media technology topics and understanding with all learners and apprentices.
- Observations of other staff during meetings with employers to ensure they understand their legal duties
- Impact of online training and all related topics of training on safeguarding to learners, apprentices, employers, the Board, governors and staff
- Progress on Quality Improvement Plan Action Points

Runway Training is committed to collecting and analysing data to assess performance, identify emerging issues and areas of success, and measure the impact of corrective actions.

Specific targets for improvement will be set and regularly monitored through the SLT and Governors' meetings. An annual report on progress, success and key issues will be presented to the Governors.

18. Linked Policies

- Safeguarding and Child Protection
- ED&I and Anti-Bullying and Harassment
- Low-level Concerns
- Comments, Compliments and Complaints
- Data Protection and Information Security, and other IT-related policies
- Staff Code of Conduct
- Learner Behaviour
- Safeguarding, Prevent, Online Safety and Sexual Harassment Risk Assessments and Action Plans
- Whistleblowing

19. Legislation and Guidance

- Online Safety Act 2023
- Keeping Children Safe in Education 2025
- Working Together To Safeguard Children (2025)
- Ofcom's Online Safety Regulations
- ICO Guidance requirements
- Computer Misuse Act
- Malicious Communications Act
- Equality Act
- General Data Protection Regulation (GDPR UK) 2018 - Data Protection Act 2018, the UK's Data Use and Access Act June 2025, brings targeted amendments to the UK GDPR regime
- The Employment Rights Act (1996)
- Information sharing: advice for practitioners providing safeguarding services (April 2024)
- Prevent Duty Guidance (2023) and any subsequent amendments or updates

20. Review

This policy will be reviewed annually. Where necessary, the review will be more frequent to ensure compliance with current legislation.