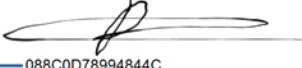



Document title:	On Line Safety Policy
Version number:	1.0
Policy Status	Approved
Date of Issue	March 23
Date of revision	n/a
Reason for revision	First implementation
Date to be revised	March 24
Policy adopted by:	<p>DocuSigned by:</p>  <p>088C0D78994844C...</p> <p>Anna Smith</p>
Policy approved by:	 <p>CharlotteWhite</p>

Scope of this Online Safety Policy

This policy applies to employees, learners, employers, volunteers, parents and carers, who have access to and are users of High Ridge Training Groups digital systems. It also applies to the use of personal digital technology on any High Ridge Training Group centre

It also outlines the commitment of High Ridge Training Group to safeguard everyone online in accordance with statutory guidance and best practice. Training Providers should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

High Ridge Training Group will deal with such incidents within this policy and associated behaviour and anti-bullying policies.

Responsibilities

To ensure the online safeguarding of all individuals it is important that everyone works 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. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within High Ridge Training Group

Senior leaders

- Senior Leaders have a duty of care for ensuring the safety (including online safety) of all individuals and fostering a culture of safeguarding.
- Senior Leaders should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- Senior leaders are responsible for ensuring that staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- Senior leaders will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal online safety monitoring role.

Online Safety Lead (Group DSL)

The Online Safety Lead will:

- work closely on a day-to-day basis with the High Ridge Training Groups Designated Safeguarding Leads (DSL's)
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide sources of training and advice for staff/employers/learners etc
- report regularly to the senior leadership team.
- liaise with the local authority/relevant body as necessary

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming

- online bullying.

Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme
- A mapped cross-curricular programme
- through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

Teaching and support staff

Staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood the staff acceptable use policy and agreement
- they immediately report any suspected misuse or problem to their groups DSL for investigation/action, in line with safeguarding procedures
- all digital communications with learners should be on a professional level and only carried out using official systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc, during teaching and other activities and implement current policies regarding these devices
- During teaching where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where teaching take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including outside of work and in their use of social media.

Technical staff

Technical staff are responsible for ensuring that:

- they are aware of and follow the High Ridge Training Group Online Safety Policy to carry out their work effectively in line with High Ridge Training Group policy
- technical infrastructure is secure and is not open to misuse or malicious attack
- High Ridge Training Group meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body
- there is clear, safe, and managed control of user access to networks and devices

- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Group DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in High Ridge Training Group policies

Learners

- are responsible for using High Ridge Training Group digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies and realise that High Ridge Training Groups Online Safety Policy covers their actions outside of their programme, if related to their membership of High Ridge Training Group

Online Safety Policy

The Online Safety Policy:

- sets expectations for the 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 High Ridge Training Group and how they should use this understanding to help safeguard learners in the digital world
- describes how the High Ridge Training Group 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
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication
- is published on the High Ridge Training Group website.

Acceptable use

The High Ridge Training Group has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the High Ridge Training Group. The acceptable use agreements will be communicated/re-enforced through:

- learner handbook
- employer handbook
- staff induction and handbook
- posters/notices around where technology is used
- built into education sessions
- High Ridge Training Group website
- peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering 					X
Users shall not undertake activities that might be classed as cyber-crime under the	<ul style="list-style-type: none"> • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to High Ridge Training Group networks, data and files, through the use of computers/devices 					X

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal	
Computer Misuse Act (1990)	<ul style="list-style-type: none"> • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) 					
Users shall not undertake activities that are not illegal but are classed as unacceptable in High Ridge Training Group policies:	Accessing inappropriate material/activities online in a High Ridge Training Group setting including pornography, gambling, drugs. (Informed by the High Ridge Training Group's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination					X
	Using High Ridge Training Group systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the High Ridge Training Group				X	
	Infringing copyright					X
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the High Ridge Training Group or brings the High Ridge Training Group into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes :	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to High Ridge Training Group								
Use of mobile phones for learning at High Ridge Training Group								
Use of mobile phones in social time at High Ridge Training Group								

Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in High Ridge Training Group, or on High Ridge Training Group network/wi-fi								
Use of High Ridge Training Group e-mail for personal e-mails								

When using communication technologies, the High Ridge Training Group considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the High Ridge Training Group
- any digital communication between staff and learners (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the High Ridge Training Group and its community
- users should immediately report to a nominated person – in accordance with the High Ridge Training Group policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- relevant policies and permissions should be followed when posting information online e.g., High Ridge Training Group website and social media. Only High Ridge Training Group e-mail addresses should be used to identify members of staff and learners.

See also Learner handbook for learner acceptable use agreement and Staff Acceptable Use Policy and Agreement

Reporting and responding

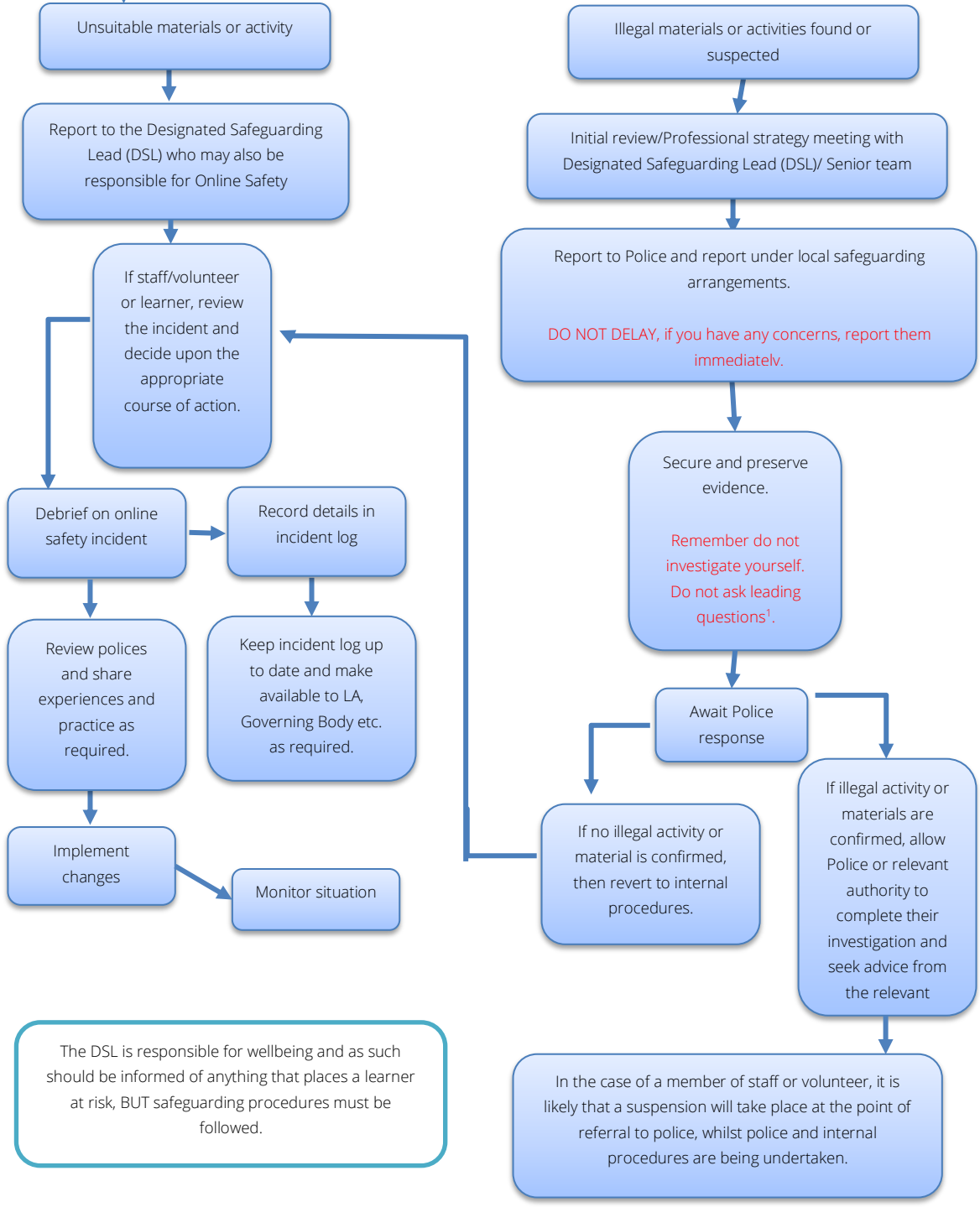
High Ridge Training Group will take all reasonable precautions to ensure online safety for all High Ridge Training Group users but recognises that incidents may occur inside and outside of High Ridge Training Group (with impact on High Ridge Training Group) which will need intervention. High Ridge Training Group will ensure:

- there are clear reporting routes which are understood and followed by all members of High Ridge Training Group which are consistent with High Ridge Training Group safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of High Ridge Training Group community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead (Group DSL) and other responsible staff have appropriate skills and training to deal with online safety risks.

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart below AND Appendix 2), the incident must be escalated through the agreed High Ridge Training Group safeguarding procedures.
- any concern about staff misuse will be reported to the group DSL, unless the concern involves the Group DSL, in which case the complaint is referred to the High Ridge Training Group Director or alternative DSL within the group
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
 - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement by local authority
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged. See template reporting log - appendix 2
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - staff, through regular briefings
 - learners, through teaching/newsletters/website
 - parents/carers, through High Ridge Training Group social media, website
 - local authority/external agencies, as relevant

High Ridge Training Group will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident Flowchart



High Ridge Training Group actions

It is more likely that High Ridge Training Group will need to deal with incidents that involve 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 High Ridge Training Group are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to tutor	Refer to DSL	Refer to Senior Leaders	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers (where appropriate)	Remove device/network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X	X	X	X		X
Attempting to access or accessing High Ridge Training Group network, using another user's account (staff or learner) or allowing others to access High Ridge Training Group network by sharing username and passwords		X	X			X		X	
Corrupting or destroying the data of other users.		X	X			X	X		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X		X			X
Unauthorised downloading or uploading of files or use of file sharing.		X	X			X		X	
Using proxy sites or other means to subvert the High Ridge Training Group's filtering system.		X	X			X		X	

Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material.		X	X			X		X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X	X	X		X			X
Unauthorised use of digital devices (including taking images)	X	X	X			X		X	
Unauthorised use of online services	X	X	X			X		X	
Actions which could bring the High Ridge Training Group into disrepute or breach the integrity or the ethos of the High Ridge Training Group.		X	X			X		X	
Continued infringements of the above, following previous warnings or sanctions.		X	X	X		X	X		X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to DSL/ Senior Leader	Refer to local authority/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X	X		X	X
Deliberate actions to breach data protection or network security rules.		X					X	X
Deliberately accessing or trying to access offensive or pornographic material		X					X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X			X	X
Using proxy sites or other means to subvert High Ridge Training Group's filtering system.		X					X	X
Unauthorised downloading or uploading of files or file sharing	X	X			X	X		
Breaching copyright or licensing regulations.	X	X				X		
Allowing others to access High Ridge Training Group network by sharing username and passwords or attempting to access or accessing High Ridge Training Group network, using another person's account.	X	X			X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X						X

Using personal e-mail/social networking/messaging to carry out digital communications with learners		X						X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X						X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X				X		
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring High Ridge Training Group into disrepute or breach the integrity or the ethos of High Ridge Training Group.		X					X	X
Failing to report incidents whether caused by deliberate or accidental actions		X	X				X	X
Continued infringements of the above, following previous warnings or sanctions.		X		X			X	X

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of High Ridge Training Group's online safety provision. Learners need the help and support of High Ridge Training Group to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- A curriculum that incorporates online safety and regularly taught in a variety of contexts.
- Teaching that builds on prior learning
- Learner need and progress are addressed through effective planning and assessment
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to all learners including those with additional learning needs or those with English as an additional language.

- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside High Ridge Training Group
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- during teaching where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Contribution of Learners

High Ridge Training Group acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for High Ridge Training Group and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- learners contribute to the online safety education programme

Staff

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of High Ridge Training Group's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand High Ridge Training Group online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings
- the DSL will provide advice/guidance/training to individuals as required.

Technology

High Ridge Training Group is responsible for ensuring that high Ridge Training Group infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. High Ridge Training Group should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

- High Ridge Training Group filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- High Ridge Training Group manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre [Appropriate filtering](#).
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- filtering logs are regularly reviewed and alert High Ridge Training Group to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through High Ridge Training Group network, content is managed in ways that are consistent High Ridge Training Group policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with High Ridge Training Group policy and practice.

Monitoring

High Ridge Training Group has monitoring systems in place to protect the High Ridge Training Group, systems and users:

- High Ridge Training Group monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice

- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

High Ridge Training Group follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and High Ridge Training Group systems through the use of the appropriate blend of strategies strategy informed by High Ridge Training Group's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- where possible, High Ridge Training Group technical staff regularly monitor and record the activity of users on High Ridge Training Group technical systems

Technical Security

High Ridge Training Group technical systems will be managed in ways that ensure that High Ridge Training Group meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of High Ridge Training Group technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- all users have clearly defined access rights to High Ridge Training Group technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all High Ridge Training Group networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password
- passwords should be long.
- The High Ridge Training Group Director is responsible for ensuring that all software purchased by and used by the High Ridge Training Group is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in [place](#) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of High Ridge Training Group systems and data. These are tested regularly. High Ridge Training Group infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee tutor, etc) onto High Ridge Training Group systems

- an agreed policy is in place regarding the extent of personal use that users (staff / learners) and their family members are allowed on High Ridge Training Group devices that may be used out of High Ridge Training Group
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on High Ridge Training Group devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on High Ridge Training Group devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Mobile technologies

High Ridge Training Group acceptable use agreements for staff and learners outline the expectations around the use of mobile technologies.

High Ridge Training Group allows:

	High Ridge Training Group devices		Personal devices		
	High Ridge Training Group owned for individual use	High Ridge Training Group owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in High Ridge Training Group	Yes	Yes	Yes	Yes	No
Full network access	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	Yes	Yes

High Ridge Training Group has provided technical solutions for the safe use of mobile technology for High Ridge Training Group devices/personal devices:

- All High Ridge Training Group devices are controlled through the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- High Ridge Training Group has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices

- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a High Ridge Training Group location or by an authorised user.
- All High Ridge Training Group devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- Devices may not be used in tests or exams
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices
- Confiscation and searching (England) - the High Ridge Training Group has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted
- The software/apps originally installed by High Ridge Training Group must remain on the High Ridge Training Group owned device in usable condition and be easily accessible at all times. From time to time High Ridge Training Group may add software applications for use in a particular teaching session. Periodic checks of devices will be made to ensure that users have not removed required apps
- High Ridge Training Group will ensure that devices contain the necessary apps for work. Apps added by the High Ridge Training Group will remain the property of High Ridge Training Group and will not be accessible to learners on authorised devices once they leave the High Ridge Training Group. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in teaching sessions in accordance with tutor direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances that has been approved
- Printing from personal devices will not be possible

Social media

High Ridge Training Group provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published

- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

High Ridge Training Group staff should ensure that:

- no reference should be made in social media to learners or High Ridge Training Group staff
- they do not engage in online discussion on personal matters relating to members of High Ridge Training Group community
- personal opinions should not be attributed to High Ridge Training Group
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official High Ridge Training Group social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under High Ridge Training Group disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, High Ridge Training Group it must be made clear that the member of staff is not communicating on behalf of High Ridge Training Group with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon High Ridge Training Group are outside the scope of this policy
- where excessive personal use of social media in High Ridge Training Group is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of public social media

- As part of active social media engagement, High Ridge Training Group may proactively monitor the Internet for public postings about High Ridge Training Group
- High Ridge Training Group should effectively respond to social media comments made by others according to a defined policy or process

Please also see our Social Media Policy

Digital and video images

High Ridge Training Group will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- High Ridge Training Group may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff must be aware of those learners whose images must not be taken/published. Those images should only be taken on High Ridge Training Group devices. The personal devices of staff should not be used for such purposes
- staff are allowed to take digital/video images to support educational aims, but must follow High Ridge Training Group policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- images will be securely stored in line with the High Ridge Training Group retention policy
- learners' work can only be published with the permission of the learner.

Online Publishing

High Ridge Training Group promotes through:

- Public-facing website
- Social media
- Online newsletters

High Ridge Training Group website is managed internally. High Ridge Training Group ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of High Ridge Training Group calendars and personal information – ensuring that there is least risk to members of the High Ridge Training Group community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The High Ridge Training Group public online publishing provides information about online safety e.g., publishing the High Ridge Training Groups Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the High Ridge Training Group website.

The website includes an online reporting process to register issues and concerns to complement the internal reporting process

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

High Ridge Training Group:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. High Ridge Training Group 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies
- provides staff and learners with information about how High Ridge Training Group looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject,
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected
- device will be protected by up-to-date endpoint (anti-virus) software

- data will be securely deleted from the device, in line with High Ridge Training Group policy once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within High Ridge Training Group
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in High Ridge Training Group
- only use encrypted data storage for personal data
- will not transfer any High Ridge Training Group personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

See also Data Protection and Confidentiality Policy

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff and learners; and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to High Ridge Training Group leadership
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

This policy should be read in conjunction with the following policies:

- Safeguarding policy
- Prevent policy
- Social Media Policy
- Anti Bully and Harassment Policy
- Password Policy
- Privacy and Cookies Policy
- Data Protection and Confidentiality Policy
- Document Retention Policy

- Plagiarism Policy
- Remote Learning Policy
- Learner and employer handbooks
- Learner disciplinary policy
- Technical Security Policy
- Staff Acceptable Use Policy and User Agreement
- Appendix 1 (below)

Appendices

The below appendices are as follows:

- A1 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A1 Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:
 Date:
 Reason for investigation:

Details of first reviewing person

Name:
 Position:
 Signature:

Details of second reviewing person

Name:
 Position:
 Signature:

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

