Safeguarding in a Digital World

POLICY LEAD (SMT Member)	Mrs Julie Ritson
REVISION STATUS (Annual)	2nd August 2021
VERSION STATUS (V)	*We reserve the right to update this policy if any changes in legislation or ESFA update deems it necessary, a numbered 'Version' would be used to ensure the up to date copy is issued.*
ANNUAL REVIEW DATE	1st August 2022
APPROVED BY COMPANY DIRECTORS	Mrs Julie Ritson and Mrs Gail Dalton-Ayres 

CONTENTS

Introduction

The development and expansion of the use of ICT, and particularly the internet, has transformed training in recent years. Young people will need to develop high-level ICT skills, not only to

maximise their potential use as a learning tool but also prepare themselves as lifelong learners and for employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. BL Training has made a significant investment both financially and physically, to ensure these technologies are available to staff and learners. The benefits are perceived to 'outweigh the risks.' However, BL Training takes very seriously their responsibility of creating a safe ICT environment for both learners and staff and has worked alongside BECTA to implement our technologies. We intend to educate learners by teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. We intend through this policy to ensure we meet our statutory obligations to ensure that learners are safe and protected from potential harm both within and outside of BL Training.

We are expected to evaluate our level of e-safety within our Self Assessment Report and will be subject of intense scrutiny by Ofsted Inspectors during our inspection.

It is important that this policy is used in conjunction with other BL Training policies (e.g., Harassment & Bullying, Safeguarding Young People & Child Protection, Prevent Duty Policy, Cyber Essential scheme, and Data Protection Policies etc.)

This policy will be reviewed by the Quality Team annually

Scope of the Policy

This policy applies to all staff, volunteers, visitors, and learners who have access to and are users of BL Training ICT systems both in and out of BL Training. Disciplinary penalties for inappropriate behaviour may be imposed. This is pertinent to incidents of cyberbullying, or any other e-safety incidents covered by this policy, which may take place outside of BL Training but is linked to BL Training.

BL Training will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will where necessarily inform parents/carers of incidents of inappropriate e-safety behaviour that takes place outside of BL Training.

Prevent Duty

Learners and staff are briefed during induction about how to stay safe when using the Internet and are encouraged to recognise that people are not always who they say they are online. They are taught to seek help if they are upset or concerned about anything they read or see on the Internet.

Inappropriate websites are banned and cannot be accessed from BL Training Limited premises

Roles and Responsibilities

Safeguarding Director/Senior Managers:

- The Safeguarding (E-Safety) Director (Julie Ritson) is responsible for ensuring the safety (including e-safety) of BL Training, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Coordinator (Safeguarding Manager Jude Speed).

- The Safeguarding (E-Safety) Director/ Senior Managers are responsible for ensuring the E-Safety Coordinator, and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues as relevant.

- The Safeguarding (E-Safety) Director/ Senior Managers will ensure that there is a system in place to allow for monitoring and support of those in BL Training who carry out the internal e-safety system monitoring role. This is to provide a safety net and support to those staff members who take on important monitoring roles.

- BL Training will monitor the Netsweeper filter for inappropriate internet content searches concerns will be forwarded to the E-Safety Manager

- The Safeguarding (E-Safety) Director and other Senior Managers must be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a staff member. (See flow chart on dealing with e-safety incidents).

E-Safety Coordinator

- Takes the overall responsibility for e-safety issues and has a leading role in establishing and reviewing BL Training E-Safety Policies/Documents.

- Ensures all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- Provides training and advice for staff.

- Liaises with the Local Authority.

- Liaises with technical staff (Smart IT).

- Will deal with investigation/action/sanctions.

Smart IT (External ITC contractor)

- Smart IT is responsible for ensuring:

- BL Training ICT infrastructure is secure and is not open to misuse or malicious attack

- That BL Training meets the e-safety technical requirements outlined in BL Training's COMP 072 New staff information & declaration form.

- Users may only access BLT's networks properly enforced password protection.

- That they keep up to date with e-safety technical information, to effectively carry out their e-safety role and to inform and update as relevant.

- That the use of the network/remote access/e-mail is regularly monitored so that any misuse/attempted misuse can be reported to the E-Safety Coordinator for investigation/action/sanctions.

- That monitoring software/systems are implemented and updated as agreed with BL Training.

ECORDIA
Are responsible for hosting our E-Portfolio system, which includes our Virtual Learning Environment (VLE) and SMS messaging system for learners. All issues are reported to the E-Safety Coordinator. The system password is protected.

Training staff and volunteers
Are responsible for ensuring that:

- They have read, understood, and signed BL's COMP 072 New Staff Information & Declaration

- They report any suspected misuse or problem to the E-Safety Coordinator for investigation/action/sanction.

- Digital communications with learners (email /Virtual Learning Environment VLE) should be on a professional level and only carried out using official BL Training systems.

- E-safety issues are embedded in all aspects of training activities.

- Learners understand and follow BLT's e-safety guidelines and ASS017 Learner acceptable use within the commitment statement part B

- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor ICT activity in sessions.

- They are aware of e-safety issues related to the use of mobile phones, cameras, and handheld devices and that they monitor their use and implement current BL Training policies about these devices.

- In sessions where internet use is pre-planned learners should use only the sites which have been checked for their suitability for their use and marked with BL's safeguarding approved symbol.

Quality Team

Members of the Quality Team will assist the E-Safety Coordinator with:

- The production/review/monitoring of BL Training Policies/documents

Learners

- Are responsible for using BLT's ICT systems in accordance with the ASS017 Learner acceptable use within the commitment statement part B which they will be expected to sign before being given access to BLT's systems.

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Will be expected to know and understand BL's policies on the use of mobile phones, digital cameras, and handheld devices. They should also know and understand BL's policies on taking /use of images and on cyberbullying.

- Should understand the importance of adopting good e-safety practice when using digital technologies outside of training and realise that BL's Policy covers their actions out of BL Training if related to their being a part of BL Training Systems.

Policy Statements

Education – Learners

While regulation and technical solutions are very important; their use must be balanced by educating learners to take a responsible approach. The education of learners is, therefore, an essential part of BL Training's e-safety provision. Learners need the help and support of BLT to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- Guidance during ICT sessions on how to use ICT in a safe manner and regularly be revisited – this will cover both the use of ICT and new technologies in and outside of BL Training

- Key e-safety messages should be reinforced as part of lesson plans, tutorials, and review activities

- Learners should be taught in all ICT sessions to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

- Learners should be helped to understand the need for the Learner acceptable use within their ASS 017 commitment statement part B and encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both in and outside of BL Training

- Learners should be taught to acknowledge the source of information used and to respect copyright when using materials accessed on the internet

- Staff should act as good role models in their use of ICT, the internet, and mobile devices

Education- Training Staff

It is essential all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training is part of all staffs' Staff Development Plans. A self-evaluation of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-safety training as part of their staff appraisal process.

- All new staff will receive e-safety training as part of their induction programme ensuring that they understand the acceptable use guidelines in the COMP072 new staff information & declaration form

- The E-Safety Manager / E-Safety Director will provide advice/guidance/training to staff as required

Technical – Infrastructure / Equipment and Monitoring

BL Training will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that Smart IT and BL Training will be effective in carrying out their e-safety responsibilities.

- BL Training ICT systems will be managed in ways that ensure that BL meets the e-safety technical requirements outlined in acceptable use guidelines in the COMP072 new staff information & declaration form

- There will be regular reviews and audits of the safety and security of BL's ICT systems alongside of Cyber essential scheme

- Servers, wireless systems, and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to BL Training ICT systems.

- All staff will be provided with a username and password by BL Training, who will keep an up-to-date record of users and their passwords

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their logon details and must immediately report any suspicion or evidence there has been a breach of security

- Users will report any actual/potential e-safety incident to the E-Safety Coordinator.

- Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, workstations, handheld devices etc. from accidental or malicious attempts which might threaten the security of BL Training systems and data.

- BL Training infrastructure and individual workstations are protected by up-to-date virus software

- Personal data can not be sent over the internet or taken off the BLT site unless safely encrypted or otherwise secured. (See BLT Data Protection Policy)

Schemes of Work
E-Safety should be a focus in all areas of the Scheme of Work and staff should reinforce e-safety messages in the use of ICT across the Scheme of Work

- In sessions where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use. Sites used within the Schemes of Work are checked for suitability and are marked with BLT's safeguarding approved symbol.

- Where learners are allowed to freely search the internet, e.g., using search engines, staff should be vigilant in monitoring the content of the websites visited. Laptops have Netsweeper filter to prevent inappropriate internet searches.

- Learners should be taught in all sessions to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

- Learners should be taught to acknowledge the source of information used and to respect copyright when using materials accessed on the internet.

Use of Digital and Video Images-
Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners' instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. BLT will educate users about these risks and will implement policies to reduce the likelihood of the potential harm

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use sharing, publication, and distribution of images. They should recognise the risks attached to publishing their images on the internet, e.g., on social networking sites.

- Staff members are allowed to take digital/video images to support training aims but must follow BL training policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on BL's equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or BL into disrepute.

- 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 good practice guidance on the use of such images.

- Learners should sign a declaration as part of their learning plan, permitting for images to be used within our marketing material.

Data Protection

Personal data will be recorded, processed transferred and made available according to the Data Protection Act 2018, which states 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 following the data subject's rights

- Secure
- Only transferred to others with adequate protection

BL Training has in place a comprehensive Data Protection Policy see this for further information regarding company data protection policy

Communications

When using communication technologies, BL Training considers the following as good Practice:

- Learners may only use mobile phones during breaks or with the permission of a staff member during their training session or unless the planned session involves interaction with mobile phones.

- BL official email service may be regarded as safe and secure and is monitored.

- Users must immediately report, to the E-Safety Coordinator (Safeguarding Manager) by following BLT policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communications between staff and learners (e.g., email, chat, VLE, etc.) must be professional in tone and content. These communications must only take place on official BL Training systems, social media sites and equipment. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

- Learners must be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the BL website, and only official email addresses should be used to identify staff.

Social Media

When using social networking sites, it is important that BL Training learner and employees feel safe and free from harassment, intimidation, and bullying, including online bullying. Any misuse of social media that has a negative impact on BL Training will be regarded as a disciplinary offence and will be investigated in line with the disciplinary procedure. BL Training's reputation must remain intact.

Social Media for Employees

- Employees should not post information, photographs or videos on sites that could bring BL Training, or its employers into disrepute.
- Employees must monitor the use of social media by learners and lead by example
- Consent is required from a learner prior to posting on social media achievements / celebrations of success
- Employees must not upload, post, forward or post a link which is likely to create liability civil or criminal.
- Employees must not represent their own views as being those of the company
- Employees should assume that all content can be linked back to themselves and BL Training
- Employees must observe the Equality Act and Human Rights Act and must not use any offensive, derogatory discriminatory language to cause embarrassment to BL Training

Social Media for Learners

- Learners must not use social media in a way which may bring BL Training into disrespect or compromise the safety or reputation of learners, educators, or employers.
- Learners must not upload, post, forward or post a link which is likely to create liability civil or criminal.
- Learners must observe the Equality Act and Human Rights Act and must not use any offensive, derogatory discriminatory language to cause embarrassment to BL Training
- Learners must not share any confidential information relating to BL Training, its staff, learners, or employers
- Communications on social media should be always respectful and must not infringe on the rights or privacy of others
- Learners are personally responsible for what they communicate on or through social media and must adhere to all codes of conduct.

Unsuitable/Inappropriate Activities

BLT believes that the activities referred to in this section would be inappropriate in a training context and those users, should not engage in the following activities in or outside of BL Training when using BL equipment or systems. BL policy restricts certain internet usage as follows: -

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals, or comments that relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, e.g., under the 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 the promotion of physical violence or mental harm

- Any other information which may be offensive to colleagues or breaches the integrity of BL or brings BL into disrepute
- Using BLT systems to run a private business
- Use systems, applications, websites, or other mechanisms that bypass safeguards employed by BL
- Uploading, downloading, or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer /network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that cause network congestion and hinder others in their use of the internet
- Online gambling
- Online shopping

Responding to Incidents of Misuse

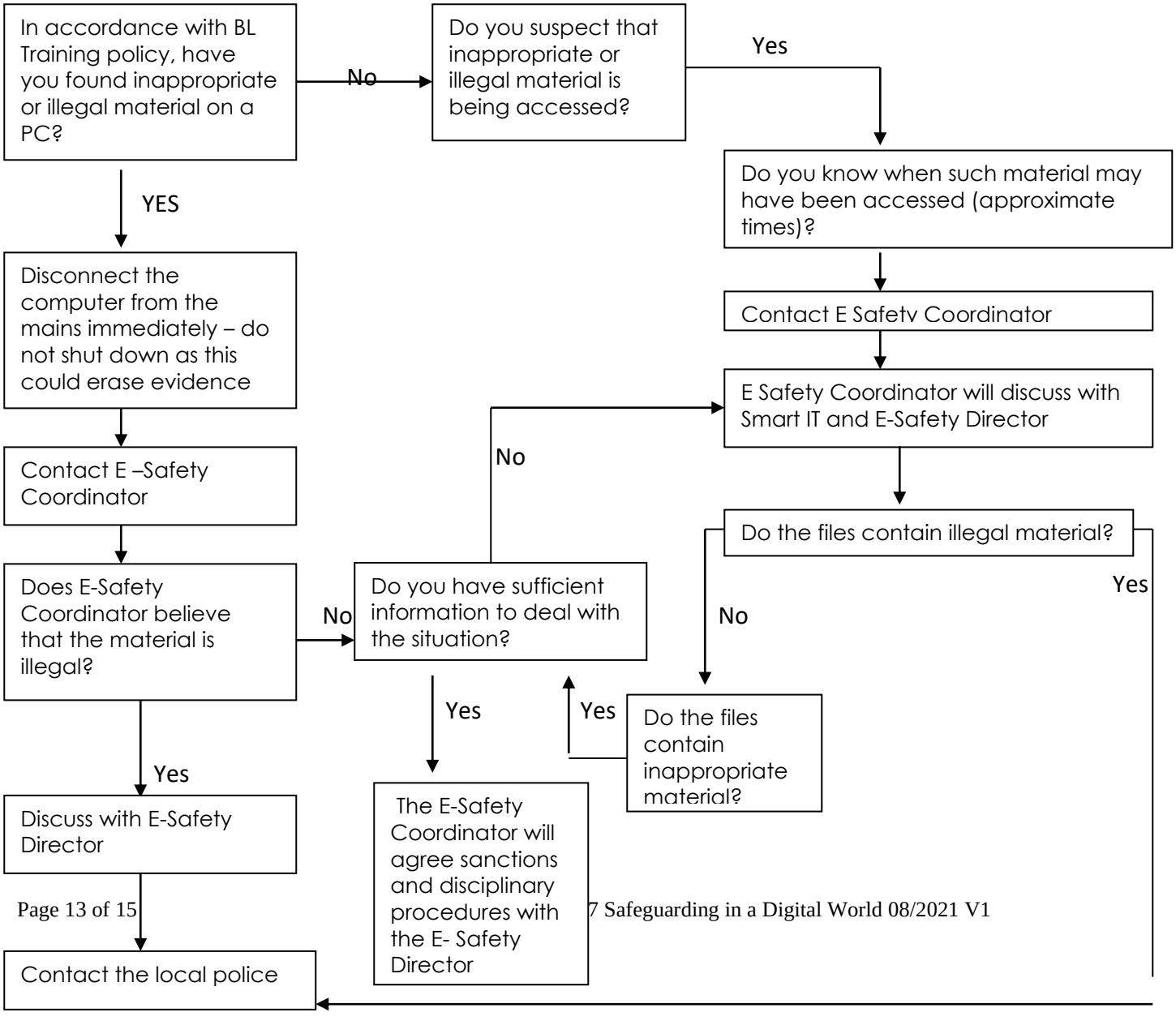
It is hoped that all staff and learners will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- Sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity, or materials

See below: -

The BL flow chart should be consulted, and actions followed in line with the flow chart the sections on reporting the incident to the police and preservation of evidence.



If members of staff suspect that misuse might have taken place, but that misuse is not illegal (as above), it is essential that the correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation.

It is more likely that BL Training 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 staff and learners are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the learner disciplinary procedures.

Learners
Incidents:

- Deliberately accessing or trying to access material that could be considered illegal (see the list in the earlier section on unsuitable/inappropriate activities)
- Unauthorised use of non-educational sites during sessions
- Unauthorised use of mobile phone/ digital camera/another handheld device
- Unauthorised use of social networking/instant messaging/personal email
- Unauthorised downloading or uploading of files
- Allowing others to access BLT network, using another learner's account
- Attempting to access or accessing BLT network using the account of a staff member
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring BL into disrepute or breach the integrity of the ethos of BL
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive pornography
- Receipt of transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Sanctions in the use of equipment or a disciplinary procedure may be followed by training staff for minor incidents. The E-Safety Coordinator will be consulted in the event of more serious incidents and where necessary will be discussed with the E-Safety Director. Illegal incidents will be reported to the police.

Staff
Incidents:

- Deliberately accessing or trying to access material that could be considered illegal (see the list in the earlier section on unsuitable/inappropriate activities).

- Excessive or inappropriate personal use of the internet / social networking sites/instant messaging/personal email
- Unauthorised downloading or uploading of files
- Allowing others to access BL network by sharing username and passwords or attempting to access or accessing BL network, using another person's account
- Careless use of personal data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking/ instant messaging / text messaging to carry out digital communications with learners
- Actions which could compromise the staff member's professional standing
- Actions which could bring BL into disrepute or breach the integrity of the ethos of BL
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

The E-Safety Director will deal with all staff incidents and where necessary issues sanctions or follow the staff disciplinary procedure.

BL Training will take all reasonable precautions to ensure users access only appropriate material. However, due to the global and connected nature of the Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a BL Training computer. BL Training cannot accept liability for the materials accessed or any consequences resulting from Internet use.

BL Training will audit ICT use from the Netsweeper filter.

Anyone requiring further guidance regarding E-Safety can receive advice from the following website www.northerngrid.org/esafety