E-Safety Policy

NTS	904
Issue Date	Oct 2014
Review Date	Jan 2021

Mission

We will increase skills through the attainment of vocational and fundamental English and maths qualifications whilst improving learners' employability skills and life chances. We aim to increase employment levels, decrease NEET and meet the skills demands of the learners, Local Authorities, employers and LEP's that we serve.

Values

Maximising learner / customer success and achievement through innovative delivery to improve individual's life chances and / or employment opportunities, in a safe, secure and nurturing environment underpinned by our specific values of:

Respect, Honesty, Trust, Openness, Equality of Opportunity for all.

Vision

Through a socially inclusive approach, we will provide high quality learning and training support, to equip individuals with the skills for future employment, further development and or Further Education.

Nova Training are committed to delivering excellence, providing the best possible experience and effective IAG for all of our learners and staff alike; with a strong emphasis on Equality and Diversity and a commitment to **Safeguarding** all of our learners / customers to ensure they feel safe, and are safe. We aim to be a high-performing organisation with a passion for learning and a dedication to become the training provider of choice.

Contents

Annex A; On-line Safety – Page 24

Introduction and Overview

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation – technology often provides the platform that facilitates harm. An effective approach to online safety empowers an organisation like Nova Training to protect and educate their staff, learners and partners in the use of technology and establishes mechanisms to identify intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three 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 courses harm

Education Providers in England and Wales are required “to ensure learners are safe from terrorist and extremist material when accessing the internet whilst in education, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore, it expects that providers “assess the risk of [their] learners being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”. There are a number of self-review systems (eg www.360safe.org.uk) that will support a school or provider in assessing their wider online safety policy and practice.

Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ (2016- with 2018 updates) obliges schools, colleges and education providers in England to “ensure appropriate filters and appropriate monitoring systems are in place. Learners should not be able to access harmful or inappropriate material from the school or colleges IT system” however, providers will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what learners can be taught with regards to online teaching and safeguarding.”

.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of Nova Training be they staff or learners with respect to the use of IT-based technologies.
- Safeguard and protect the learners and staff of Nova Training.
- Assist all staff working with learners to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other Nova Training policies.
- Ensure that all members of Nova Training are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with Learners.

The main areas of risk for our Centres can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Peer on peer abuse
- Identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation

- Health and well-being (amount of time spent online (internet or gaming) (Ref CIF 2015)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

(**Ref Ofsted 2013**)

Scope

This policy applies to all members of Nova Training community (including staff, Learners, volunteers, parents / carers, visitors, community users) who have access to and are users of Nova Training ICT systems, both in and out of Nova Training centres.

The Education and Inspections Act 2006 empowers Senior Managers in FE establishments to such extent as is reasonable, to regulate the behaviour of Learners when they are off Nova Training premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of Nova Training premises, but is linked to attendance at Nova Training. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by this Policy.

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

Role	Key Responsibilities
Operations Director	• To take overall responsibility for e-safety provision. • To take overall responsibility for data and data security. • To ensure the company uses an approved, filtered internet service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Safeguarding Team. • To ensure that there is a system in place to monitor and support staff that carry out internal e-safety procedures (e.g. Safeguarding Team).

Role	Key Responsibilities

Safeguarding Team	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the company's e-safety policies / documents.
	• Promotes an awareness and commitment to e-safety throughout the organisation.
	• Ensures that e-safety education is embedded across all curriculums.
	• Liaises with ICT technical staff where necessary.
	• To communicate regularly with the Senior Management Team to discuss current issues, review incident logs and filtering / change control logs.
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
	• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date.
	• To ensure the security of the company's ICT system.
	• To ensure that access controls / encryption exist where required to protect personal and sensitive information held on company owned devices.
	• To ensure the company's policy on web filtering is applied and updated on a regular basis.
	• To ensure that an e-safety incident log is kept up to date/safeguarding log.
	• Facilitate training and advice for staff.
	• Liaise with Local Authorities and relevant agencies in the areas where Nova Training premises are located.
	• Are regularly updated in e-safety issues and legislation, and aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media
	• That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Operations Director / HR Manager for investigation / action / sanction.
	• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
	• To keep up-to-date documentation of the company's e-security and technical procedures.
	• To ensure that all data held on learners on company machines used in administrative functions have appropriate access controls in place.

Role	Key Responsibilities
Senior Management Team	• To ensure that the company follows all current e-safety advice to keep the learners and staff safe (Prevent). • To approve the e-safety policy and review the effectiveness of the policy. This will be carried out by receiving regular information about e-safety incidents and monitoring reports. • To support the company in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the Designated Senior Safeguarding Lead will include regular review of safeguarding incident logs, display of e-safety promotional material in centres. • To ensure that users may only access the company's networks through an authorised and properly enforced password protection policy.
Internal Quality Assurance Verifiers	• To oversee the e-safety element in the curriculums we deliver. • To liaise with the Quality Improvement Manager regularly.
Quality Improvement Manager	• To report any e-safety related issue that arises to the Safeguarding Team. • That he / she keeps up to date with the company's e-safety policy and technical information in order to effectively carry out e-safety audits as part of the QI function and to inform and update others as relevant.
Management Information Services	• To ensure that all data held on learners on is fully protected in line with the requirements of the General Data Protection Regulation
Teachers, Trainers and Apprenticeship Coaches	• To embed e-safety issues in all aspects of the curriculum and other learning and enrichment activities. • To supervise and guide learners carefully when engaged in learning activities involving online technology (including, extra-curricular and extended activities if relevant) • To ensure that learners are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All Staff	• To read, understand and help promote the company's e-safety policies and guidance • To read, understand, sign and adhere to the company Acceptable Use Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current company policies with regard to these devices • To report any suspected misuse or problem to the centre e-safety Champion or Manager • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology

Role	Key Responsibilities
	• To ensure that any digital communications with learners should be on a professional level and only through company based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Learners	• Read, understand, sign and adhere to the Learner Acceptable Use Policy. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand company policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand company policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of centre and realise that the company's E-Safety Policy covers their actions out of centre, if related to their attendance at a company centre. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in centre and at home • To help the company in the creation / review of e-safety policies through the Learner Voice meetings and other events.
Parents/carers	• To support the company in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the learners' use of the internet and Nova's use of photographic images and video footage. • To read, understand and promote the Learner Acceptable Use Agreement with their children. • To consult with the company if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within the company or belonging to the company and used off-site.

Communication:
The policy will be communicated to staff / learners / partners in the following ways:

- Policy to be posted on the company website / available on the company Intranet / displayed in centres / classrooms.
- Policy to be part of induction pack for new staff.
- Acceptable use agreements discussed with learners joining programmes of learning run by the company.
- Acceptable use agreements to be held in learner files and staff personnel files.

Handling complaints:

The company will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a company computer or mobile device. The company cannot accept liability for material accessed, or any consequences of internet access.

Staff and learners are given information about infringements in use and possible sanctions. Sanctions may include:

- Interview/counselling by tutor / Centre Manager / Programme Operations Manager/ HR Manager.
- Informing parents or carers.
- Removal of internet or computer access for a period (which could ultimately prevent access to files held on the system, including examination coursework).
- Referral to MASH / Police.

Our Centre Managers act as first point of contact for any complaint. Any complaint about staff misuse is referred to the HR Department.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with by the Safeguarding Team in accordance with Safeguarding procedures.

Review and Monitoring

The e-safety policy is referenced from within other Company policies: such as the Safeguarding Policy

- The Company has a Data Protection Manager/ e-Safety Manager who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use by the Company
- The e-safety policy has been written by the company's Senior Safeguarding Lead and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed and approved by the SMT. All amendments to the e-Safeguarding policy will be discussed in detail by the Safeguarding Team and with all members of staff.

2. Learning and Curriculum

Learner e-safety curriculum

The company has a clear, progressive e-safety education programme as part of its curriculums. It is built on the e-safeguarding and e-literacy framework national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- To understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behavior when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- [for older learners] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline, or the CLICK CEOP button.
- Plan for internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind Learners about their responsibilities through an end-user Acceptable Use Agreement which every Learner will sign and which will be displayed throughout the Company's premises
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and Learners understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and Learners understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and Manager Training

The Company will:

- Ensure staff will not send or receive sensitive and personal data via email and understand the requirement to protect data where the sensitivity requires data protection in line with the GDPR.
- Make regular training available to staff on e-safety issues and the company's e-safety education program via annual updates, operations meetings, case review meetings and learner voice meetings.
- Provides, as part of the induction process, all new staff (including those on university / college placement and work experience) with information and guidance on the e-safety Policy and the company's Acceptable Use Policies.

Parent Awareness and Training

The Company will make available as necessary advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to ensure that principles of e-safe behaviour are made clear.
- Information leaflets, in learner newsletters and on the company web site.
- Via demonstrations, practical sessions held in centres.
- Suggestions for safe Internet use at home.
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident Management

Expected Conduct

In the Company, all users:

- Are responsible for using ICT systems in accordance with the relevant Acceptable Use Policy when given access to company IT systems.

- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of centre and realise that the company's e-safety Policy covers their actions out of centre, if related to their attendance on a course of learning or other activity provided by the company.
- Will be expected to know and understand the company's policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Nova policies on the taking / use of images and on cyber-bullying

Staff

- Are required to read the Company's e-safety policy and using the Company's ICT systems accordingly, including the use of mobile phones, and hand held devices.

Learners

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

Parents/Carers

- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

Within the Company:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All staff, learners and our wider communities if involved in enrichment activities are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the Company's due processes.
- Support is actively sought from other agencies as needed (e.g. the Local Authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the Company. All relevant records are reviewed / audited and reported to the SMT and may be shared with other agencies as deemed appropriate and necessary.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or Learners receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the IT infrastructure

Internet access, security (virus protection) and filtering

The Company:

- Has filtered secure broadband connectivity;
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network health through use of anti-virus software and has the network set-up so staff and learners cannot download executable files;
- Uses secured intranet email to send personal data between centre and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked Learner access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with a registered company, RGL, to ensure any concerns about the system are communicated so that systems remain robust and protect Learners;
- Is vigilant in its supervision of Learner's use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where Learners of various ages have access;
- Ensures all staff and Learners have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures Learners only publish within an appropriately secure environment such as the Company's learning environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the Company's Learning intranet as a key way to direct Learners to age / subject appropriate web sites; Plans the curriculum context for Internet use to match Learners' ability, using Google Safe Search
- Is vigilant when conducting 'raw' image search with Learners e.g. Google image search;
- Informs all users that Internet use is monitored;

- Informs staff and learners that that they must report any failure of the filtering systems directly to RGL as our service provider. Our system administrator logs or escalates failures to RGL as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff induction, operations meetings and the CPD programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying that may from time to time be discovered by learners and staff.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  The Company;
  - Uses individual, audited log-ins for all users;
  - Uses guest accounts occasionally for external or short term visitors for temporary access restricted to appropriate services
  - Has additional local network auditing software installed;
  - Ensures the Senior Safeguarding Lead is up-to-date with policies and requires the Technical Support Provider, RGL, to be up-to-date with the Company's services and policies;
  - Storage of all data within the Company will conform to the UK data protection requirements

    Learners and Staff using mobile technology, where storage of data is online, will conform to the GDPR at all times

To ensure the network is used safely, the Company:

- Ensures all staff read and that they have understood the Company's e-safety Policy. New staff are set-up with network access, internet access and email access. Online access to service is through a unique, audited username and password;
- Ensures that staff access to the Company's PICS management information system is controlled through a separate password for data security purposes;
- Will provide Learners with an individual network log-in username and personal password.
- Makes clear that no one should log on as another user and makes it clear that Learners should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions than a learner log-in and inappropriate use could damage files or the network;

- Has set-up the network with a shared work area for learners and one for staff. Staff and learners are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended. When terminals are left unattended or unused for 2 minutes they revert to a sign-on screen automatically;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 2 minutes of inactivity and have to re-enter their username and password to re-enter the network.];
- We request that teachers and learners DO NOT switch computers off at the end of the day so we can run automatic updates and usage checks and we also automatically switch off all computers at 9.00 pm to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download, social networking and/or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Does not allow staff to use private computers to access the Company's servers without the protection of an approved Access Gateway;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date. The company provides automatic anti-virus and spyware updates for all company owned computers and when linking a staff owned computer via the Access Gateway.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Company, is used solely to support their professional responsibilities and that they notify the Company of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains all IT equipment to ensure Health and Safety is followed; equipment is always installed and checked by RGL and any electrical testing is carried out as required by qualified electricians.
- Has integrated curriculum and administration networks, but access to the Management Information System/PICS is set-up so as to ensure only authorised staff users can access modules related to their role;
- Ensures that access to the Company's network resources from remote locations by staff is restricted and access is only through an approved system;

- Does not allow any outside Agencies to have access our network or part network except where there is a clear professional need and then access is restricted and is only through our security approved systems under controlled supervision;
- Provides Learners and staff with access to content and resources through the Company intranet Learning Platform which staff and Learners access using via their username and password;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for monitoring our CCTV system as set-up by our Facilities Team;
- Ensures that all Learner level data or personal data sent over the Intranet is only sent within an approved secure system.
- Our wireless network has been secured to industry standard security level and /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors/Screens are maintained so that the quality of presentation remains high;
- Reviews the Company ICT systems regularly with regard to health and safety and security.

Passwords policy

- This Company makes it clear that staff and Learners must always keep their password private, they must not share it with others and they must not leave it in written form where others can find it.
- All staff have their own unique and private passwords to access Company systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our IT system.
- We prompt staff to change their passwords into the IT system every 90 days or as requested

E-mail

The company

- Provides staff with an email account for their professional use and makes clear personal emails should be through a separate account;
- Does not publish personal e-mail addresses of Learners or staff on the company website. The exception to this would be where there is a need for a contact address such as in responding to job advertisements.
- Will contact the Police if one of our staff or Learners receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date with suitable protections against spam, phishing and virus attachments
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the Company, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent by staff to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on company headed paper;
- that forwarding 'chain' e-mail letters is not permitted
- ensures that all communications containing "PERSONAL" data are sent via registered/recorded mail services and not via email.

Learners:

- Learners are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Learners are taught about the safety and 'netiquette' of using e-mail both in a work setting and at home i.e. they are taught:

- not to give out their e-mail address unless it is to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they must immediately tell a teacher / centre manager if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

- Learners sign the Induction Plan to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Company website

- The Operations Director takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information to the website is restricted to our website authorisers:
- Most material is the Company's own copyright; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the company address, telephone number and we use a general email contact address, e.g. info@novatraining.co.uk Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use Learners' names when saving images in the file names or in the tags when publishing to the company website;
- We do not use embedded geo data in respect of stored images

Learning platform

- Uploading of information on the Company's' intranet is shared between different staff members according to their responsibilities
- Photographs and videos uploaded to the Company's intranet will only be accessible by staff members;
- In centres, Learners are only able to upload and publish within the company intranet and any approved closed systems;

Social networking

- Teachers are instructed not to run social network spaces for Learner use on a personal basis or to open up their own spaces to their Learners. Staff are instructed to use the Company's supplied mobile phones for communication with learners where they have been issued or the Company's e-mail system for communications with learners.

All staff will ensure that in private use:

- No reference will be made in social media to Learners / parents / carers or Nova staff unless permission to do so is obtained from the Operations Director prior to release of such social media
- They do not engage in any online discussion on personal matters relating to members of staff or Learners
- Personal opinions should not be attributed to the *company*
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in Company premises and transport as part of our site surveillance for staff and Learner safety. We will not reveal any recordings except where disclosed to the Police as part of a criminal investigation.
- We may use specialist lesson recording equipment on occasions as a tool to observe lessons and/or share best teaching practice. Prior to sharing such videos the company will seek the permission of those persons recorded on the videotape. In any dispute on the suitability of such material for purposes of sharing best practice or illustrating certain procedures the Operations Directors decision will be final.
- All recordings are kept for a minimum of 7 days and then overwritten unless they are copied in connection with an investigation or used as a tool to share best teaching practice.

5. Data security: Management Information System access and Data transfer

The Company operates under the ICO regulations and the GDPR legislation. It is registered with the ICO for the types of data used and processed in connection with the contracts it holds and operates in the course of its business.

The Company has a Safeguarding and Child Protection Policy (NTS717), Data Protection Policy (NTS743) and a Security Manual (NTS743a) which should be read in conjunction with this document.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought onto Company premises are entirely at the staff member, Learner's & parents' or visitors own risk. The Company accepts no responsibility for the loss, theft or damage of any phone or hand held device brought onto its premises.
- Learner mobile phones which are brought into classes must be turned off (not placed on silent) if so requested by a teacher or manager and stored out of sight during classes. They must remain turned off and out of sight until the end of the class unless being used as an educational tool.
- Staff members may use their phones during Nova break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by a Senior Manager or Centre Manager. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Operations Director is able to withdraw or restrict authorisation for use at any time if it is deemed to be necessary.
- The Company reserves the right to search the content of any mobile or handheld devices used on Company premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or learners need to contact each other during the Nova day, they should inform the teacher and/or centre manager.

- If a staff member is expecting an urgent or important personal call they may leave their phone with the centre manager to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal class time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to Nova are the responsibility of the device owner. The Company accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within Company sites, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- When on Company premises any Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher and centre manager.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Learners' use of personal devices

The Company strongly advises that Learner mobile phones should not be brought into Nova unless being used for educational purposes. However;

- The Company accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a Learner breaches this policy then the phone or device will be confiscated and will be held in a secure place by the centre manager until the Learner leaves the premises, at which time the device will be returned. Mobile phones and devices will be released to police, parents or carers in accordance with this policy if they were confiscated for purposes of investigation into bullying or other unlawful activity.
- Phones and devices must not be taken into examinations. Learners found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the Learner's withdrawal from either that examination or all examinations.

- If a Learner needs to contact his or her parents or carers during normal class times for any reason, they must advise their teacher and/or the centre manager. Parents are advised not to contact their child via their mobile phone during the Nova day, but to contact the Nova office.
- Learners should protect their phone numbers by only giving them to trusted friends and family members. Learners will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Learners maybe be provided with company mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted by the centre manager – name, make & model, serial number. Any permitted images or files taken in classes must be downloaded from the device and deleted before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting learners or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a company phone where contact with Learners, parents or carers are required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow Learners to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior management team and/or centre manager.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of Learners and will only use work-provided equipment for this purpose.
- If a member of staff breaches this policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for company duties, for instance in case of an emergency during off-site activities, or for contacting Learners or parents, then a company mobile phone will be provided and used.

In an emergency where a staff member doesn't have access to a Company-owned device, they should use their own device and if they wish to keep their personal number anonymous insert 141 before the number they are dialling.

Digital images and video

The Company:

- Will gain parental / carer permission for use of digital photographs or video involving their child as part of the agreement form when their daughter / son joins a programme of learning;
- We do not identify Learners in online photographic materials or include the full names of Learners in the credits of any published Company produced video materials / DVDs;
- Staff sign the Company's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of Learners;
- If specific Learner photos (not group photos) are used on the Company web site or in other publications the Company will obtain individual parental or Learner permission for its long term use
- The Company blocks/filters access to social networking sites or newsgroups unless it is a specific approved site for educational purposes;
- Learners are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT curriculum;
- Learners are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public their personal information.
- Learners are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or Nova. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Electronic Asset Disposal

All redundant IT equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The Company will only use RGL who, if required, will supply a

written guarantee that this will happen. The company's Security Manual (NTS743a) contains specific guidance and procedures for the secure disposal of PERSONAL classified sensitive/confidential information

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Version Control

As part of the maintenance involved with ensuring the e-safety policy is current and effective, regular revisions will be made to the document. It is important that the document user ensures the document they are using is up to date, i.e. The latest version available in drive X: **Master Documents; NTS Documents**.

Annex A: On-line safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides a platform that facilitates harm. An effective approach to online safety empowers Nova Training to protect and educate the whole organisation in the use of Information Technology and establishes mechanisms to identify, intervene in and deal effectively with any incident where appropriate.

The breadth of issues classified within on-line safety is considerable, but can be categorised into three areas of risk:

• **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Filters and monitoring

Nova Training is doing all that it can do to limit learner's exposure to the above risks from the company's IT system. As part of this process, Nova Training has put in place appropriate filters and monitoring systems.

Nova Training understands its responsibility to safeguard and promote the welfare of learners, and provide them with a safe environment in which to learn.

Whilst filtering and monitoring is an important part of the online safety picture for Nova to consider, it is only one part. Nova considers a whole organisation approach to online safety and this includes a clear policy on the use of mobile technology in all of Nova premises. Many learners have unlimited and unrestricted access to the internet via 3G and 4G in particular and Nova encourages learners to only use phones for learning and if this is not adhered to then phones are banned.

Reviewing online safety

Technology evolves and changes rapidly and there is a free online safety self-review tool which can be found via the 360 safe website. UKCCIS have recently published Online safety in schools and colleges.

Information and support	What it /provides
https://www.thinkuknow.co.uk/	NCA CEOPs advice on online safety
https://www.disrespectnobody.co.uk/	Home Office advice on healthy relationships, including sexting and pornography
https://www.saferinternet.org.uk/	Contains a specialist helpline for UK schools and colleges
https://swgfl.org.uk/products-services/online-safety/resources/	Online safety resources
https://www.internetmatters.org/	Help for parents on how to keep their children safe online
https://www.childnet.com/resources/know-it-all-secondary-toolkits/lower-secondary-toolkit/cyberbullying	Guidance and free resources on dealing with cyberbullying
https://www.pshe-association.org.uk/curriculum-and-resources	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
https://educateagainsthate.com/teachers/	Practical advice for teachers on protecting children from extremism and radicalisation.
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation	A briefing note on how social media is used to encourage travel to Syria and Iraq
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis	The UK Council for Child Internet Safety's website provides: • Sexting advice

	• Online safety: Questions for Governing Bodies • Education for a connected world framework
https://www.nspcc.org.uk/services-and-resources/working-with-schools/	NSPCC advice for schools and colleges
https://www.net-aware.org.uk/	NSPCC Guide to the social networks that children use
https://www.commonsensemedia.org/	Independent reviews, age ratings, & other information about all types of media for children and their parents
https://www.gov.uk/government/publications/searching-screening-and-confiscation	Guidance on searching children in an educational setting and confiscating items such as mobile phones

Safeguarding our learners

Prevent duty

Our key aim is to protect our learners from the risk of radicalisation and ensure that we have the appropriate support mechanisms in place in order to protect learners from this risk. As a training provider, we will:

- Ensure staff are able to identify learners who may be vulnerable to radicalisation
- Ensure staff know what to do if learners have been identified.
- Protect learners from the risk of radicalisation as part of our safeguarding duties, whether these risks come from within Nova Training or are the product of outside influences.
- Build learners' resilience to radicalisation by promoting fundamental British values and enabling learners to challenge extremist views. (We will be a safe space where learners can understand the risks associated with terrorism and develop the knowledge and skills to be able to challenge extremist arguments).
- Nova Training will assess the risk of our learners being drawn into terrorism.
- Our staff will have a general understanding of the risks affecting the learners within our community. This would include the increased risk of online radicalisation.
- Our staff will have a specific understanding of how to identify individual learners who may be at risk of radicalisation and what to do to support them.

- In line with our safeguarding policy, staff will be alert to any changes in learner's behaviour which could indicate that they may be in need of help or protection.
- As a staff, we would use our professional judgement in identifying learners who may be at risk of radicalisation and act proportionality.
- Again, as in line with our safeguarding policy, action will be taken if staff observe any behaviour that may cause concern.
- If necessary, (if we felt a learner might be vulnerable to being drawn into terrorism) we would make a referral to the Channel programme