Adult Training Network (ATN)

IT User/E-Safety Policy

Reviewed on: **1st April 2019**

Reviewed by; **S Singh Gill**
Managing Director

Next Review Date: **1st April 2020**

Contents Page Number

1. Policy Aims

The e-Safety, also known as 'online safety', policy has been written by the Adult Training Network (ATN). E-Safety is part of the safeguarding 'duty of care', which is applicable to all working in education. The aims of ATN's e-Safety policy is to:

- Safeguard and protect all members of staff, learners and those who access the services provided by ATN
- Identify methods and approaches to take in order to educate and raise awareness of e-Safety throughout ATN
- Ensure all staff are working safely and responsibly online whilst also ensuring the use professional standards and practice when using online technology
- Identify the key steps to take when dealing with an e-Safety incident or e-Safety concerns

ATN identifies that there are numerous issues to consider in regards to e-Safety. These issues can be broadly categorised into three areas of risk:

- Content: exposure to illegal, inappropriate and/or harmful material
- Contact: being subjected to harmful online interaction with other users online
- Conduct: an individual's personal online behaviour that may increase the possibility of, or causes, harm

The key areas of risk that all staff, learners and those who access services provided by ATN must be made aware of include:

- Scams (fake emails, phishing or spoofing, etc.)
- Inappropriate contacts
- Harassment and bullying, including cyber bullying
- Masquerading and identity theft
- Inappropriate materials
- Sexting and 'revenge porn'
- Inappropriate use of social media (e.g. Facebook, Twitter)
- Illegal acts by users (e.g. copyright breach)
- Malicious software (e.g. viruses and downloads)

2. Policy Scope:

- ATN believes that e-Safety and staying safe online is a crucial part of our safeguarding duty and it acknowledges the responsibility we have to ensure all staff, learners and those who access the services provided by ATN are protected from the risk of harm online.
- ATN understands and identifies that the use of the internet and other technological devices, such as computers, laptops, tablets, mobile phones and game consoles play a part in the everyday lives of staff, learners and those who access the services provided by ATN.
- ATN believes that all staff, learners and those who access the services provided by ATN should be empowered to gain an understanding of online risks and to develop strategies to manage and respond to these risks.
- ATN's e-Safety policy applies to all staff, learners and those who access the services provided by ATN. The e-Safety policy applies to all access to the internet and the use of technology, including the personal devices issued to ATN staff for use off-site such as work mobile phones.

2.1 Links with other policies and guidelines

ATN's e-Safety policy links with several other policies and guidelines that have been put into place including:

- Safeguarding policy (which incorporates the Prevent Policy of ATN)
- Guidelines for Acceptable Computer Use for Learners

3. Role and Responsibilities

ATN has appointed Sarjeet Singh Gill, as the Designated e-Safety lead. The e-Safety Lead should be immediately contacted for support regarding e-Safety or in the event of an e-Safety incident. If the e-Safety Lead is absent or is unable to perform their duties, then the Deputy e-Safety Lead should be contacted.

Name	Designation	Email Address	Telephone Number
Sarjeet Singh Gill	e-Safety Lead	sgill@adult-training.org.uk	020 8574 9588
Kamaljit Kaur	Deputy e-Safety Lead	kamaljit@adult-training.org.uk	020 8574 9588

3.1 The e-Safety Lead will:

- Annually review the e-Safety policy to ensure it is updated to follow any national or local policy requirements, any previous e-Safety concerns that were identified or any changes to the technical infrastructure
- Maintain records of e-Safety concerns and the actions that were taken
- Ensure that e-Safety and online safety is identified as a safeguarding issue and that practice complies with national and local recommendations and requirements
- Ensure that there is an updated guideline for computer use of learners
- Work with IT staff to monitor the safety and security of computer systems in place and that there is an appropriate filtering and monitoring system in place to ensure online safety
- Ensure that there is a robust reporting system in place for individuals to report any concerns regarding online safety
- Ensure that appropriate risk assessments are undertaken regarding the safe use of the internet and technology, such as computers, laptops, telephones and mobile phones.

3.2 All staff members will:

- Read and adhere to the e-Safety policy
- Contribute to the implementation of the e-Safety policy and the guidelines for computer use of learners
- Be a role model when using the internet and technology and maintain a sense of professionalism when using the internet and technology both on and off- site
- Know when and how to escalate e-Safety issues, including signposting to appropriate support
- Identify any e-Safety concerns and immediately inform the e-Safety Lead

3.3 All learners will:

- Read and adhere to the e-Safety policy and ATN's Guidelines for Acceptable Computer Use for Learners
- Take responsibility for keeping themselves and their peers safe online
- Contribute to the development of the e-Safety policy
- Seek help and support from a tutor, staff member of the e-Safety lead if there is a concern online, or if they are concerned about the online safety of others
- Respect the feelings and rights of others both on and offline

3.4 Training:

- ATN will provide and discuss the e-Safety policy with all members of staff, learners and those who access the services provided by ATN.
- ATN will provide updated and appropriate e-Safety training for staff members, learners and those who access the services provided by ATN with at least annual updates
- ATN will ensure staff, learners and those who access the services provided by ATN are reminded to behave professionally and in compliance with ATN's policies when accessing ATN's systems and devices

- ATN will highlight useful educational resources and website links which tutors should use, according to the ability of their learners
- ATN will ensure all members of staff are made aware of the procedures to adhere to regarding e-Safety concerns which affect learns, colleagues and those who access the services provided by ATN.

4. Reducing the Risks Online:

ATN recognises that the internet is a constantly changing environment with new apps, devices, websites and materials emerging constantly. Due to this, there is also an increase in the risks found online. ATN will:

- Regularly review the approaches in place which identify, assess and minimise online risks
- Examine new technologies for educational use and undertake appropriate risk assessments before ATN permits the use of it
- Ensure that appropriate filtering and monitoring systems are in place and take the necessary approaches to ensure that staff, learners and those who access the services provided by ATN can only access appropriate material
- Due to the global nature of the internet, it is not possible to guarantee that unsuitable and inappropriate material cannot be accessed via devices in the property of ATN

All members of ATN staff, learners and those that access the services provided by ATN are made aware of ATN's expectations regarding safe and appropriate online behaviour and the importance of not posting, sharing or spreading any content, comments, images or videos which could cause harm, distress or offence to other individuals.

5. Safer Use of Technology

5.1 Classroom Use

ATN uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which includes search engines
- Email

- All ATN owned devices will be used in accordance with the Guidelines for Acceptable Computer Use for Learners and with appropriate safety measures in place.
- Staff members will always evaluate websites, online tools and apps fully before using them in the classroom or recommending them to learners for use at home.
- ATN will ensure that the use of all internet-derived materials, by staff and learners, adheres to copyright law and acknowledges the source of information.
- All learners will read the Guidelines for Acceptable Computer Use for Learners and agree to its terms before being given access to ATN's computer system, IT resources or internet.

5.2 Security and Management of Information Systems

ATN will take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly
- Not downloading unapproved software to ATN's devices or opening unfamiliar email attachments
- Regularly checking files held on ATN's network
- The appropriate use of user logins and passwords to access ATN's network.
- All users should log off or lock their screens/devices if they leave the system unattended
- For further information, contact the e-Safety Lead or ATN's Network Engineer

5.2.1 Password Policy

- All members of staff will have their own username and private password to access ATN's systems; staff are solely responsible for keeping their login information safe and should not share it with others

5.2.2 Managing Personal Data Online

- Personal data will be recorded, processed, transferred, and made available online in accordance with the General Data Protection Regulation (GDPR) 2018.

5.3 Managing the Safety of the ATN Website

- ATN will ensure that our website complies with guidelines for publications including: accessibility; data protection; privacy policies and copyright
- The personal information of staff will not be published on our website; the only contact details found on the website will be the addresses of ATN offices, the telephone numbers and company emails
- The administrator account for the ATN website will be secured with a strong password
- ATN will post appropriate information about safeguarding, including the contact details for the Designated Safeguarding Team.

5.4 Managing Email

- Access to ATN email systems will always take place in accordance with GDPR legislation and in line with other ATN policies, such as Code of Conduct and Confidentiality
- It is not permitted to forward any chain/spam emails. All spam and junk emails will be blocked and will be reported to the e-Safety Lead.
- All electronic communication that contains sensitive or personal information will only be sent using secure and encrypted email
- ATN email addresses and other official contact details are not permitted to be used for setting up personal social media accounts
- ATN staff, learners and those who access the services provided by ATN will immediately inform the e-Safety Lead if they receive any offensive electronic communication, and this will be recorded by the e-Safety Lead

5.4.1 Staff

- Using personal email addresses by staff for any official ATN business is prohibited. All staff members are provided with an ATN company email address and this should be used for all official communication
- Staff are encouraged to have an appropriate work life balance when responding to email, especially if the electronic communication is taking place between staff, learners and those who access services provided by ATN

5.4.2 Learners

- Learners may access their personal email accounts on computers provided by ATN. However, this is only permitted out of class hours and learners must sign out of their accounts completely

6. Social Media

6.1 Expectations

- ATN expects all staff, learners and those who access services provided by ATN to be safe and responsible when using social media
- 'Social media' refers to (but is not limited to): blogs, wikis, social networking sites, forums, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger sites/ apps.
- ATN advises all staff, learners and those who access services provided by ATN to not publish specific and detailed private thoughts, pictures, videos or messages on any social media platforms. Specifically, content that may be considered threatening, harmful and offence to other individuals.
- If staff, learners or those who access services provided by ATN become concerned regarding the online conduct and behaviour of any individual connected to ATN, then they should raise this concern with the e-Safety Lead.

6.2 Staff Personal Use of Social Media

- The e-Safety Lead will discuss with all members of staff the safe and responsible use of social networking and social media as part of staff induction and will be revisited during staff training sessions
- ATN staff will be reminded that their online behaviour and conduct will have an impact of their reputation within ATN.
- ATN staff will be reminded that the personal messages, photos and videos they post online do not reflect the views of ATN
- All members of staff should safeguard themselves and their privacy when using social media platforms. Staff members are advised to:
    - Setting the privacy levels of their personal sites as strictly as they can
    - Be aware of location sharing services
    - Opt out of public listings when using social networking sites
    - Logging out completely of all accounts after use
    - Keeping passwords safe and change them regularly
- Staff members are advised and encouraged to not identify themselves as ATN employees on their personal social networking accounts. This is to prevent the information found on these sites from being linked to ATN and to safeguard the privacy of other staff members, learners and those who access the services provided by ATN.
- Staff members are encouraged to consider the information they share and post online. Staff should ensure that they do not post any harmful, offensive, intimidating or illegal material.
- Staff members should notify the e-Safety Lead immediately if they become aware of any content that has been shared online that poses a risk to the safeguarding of other staff, learners and those who access the services provided by ATN.

6.3 Learner Personal Use of Social Media

- Learners will be made advised on how to use social media safely and appropriately. They should refer to the Guidelines for Acceptable Computer Use for Learners for more information.
- Learners will be advised to:
    - Consider the benefits and risks of sharing personal details on social media sites which could identify who they are and their location. This includes full name, address, contact numbers, schools attended, place of work, specific interests, clubs attended, email addresses and other social media contact details
    - Only accept and invite known friends and family on social media sites and to protect their online profiles by making their accounts private or only accessible to people they know
    - Never meet anyone they meet online, especially in a private setting
    - Use safe passwords that are not shared with anyone else
    - Think about what messages, photos and videos they share online and ensure that they do not post or share any harmful, offensive, intimidating or illegal material
    - Block and report unwanted communications and notify the e-Safety Lead if they become concerned about what they have seen or received on social media sites

6.4 Official ATN Use of Social Media

- The official ATN social media channels are:
    - https://www.facebook.com/Adult-Training-Network-1655397611400772/
    - https://twitter.com/letchworthatn
- The official use of ATN social media channels only takes place with clear promotion or community engagement objectives
- Official ATN social media use will be conducted in line with existing policies, including; Safeguarding, Data Protection and Confidentiality
- The e-Safety Lead will ensure that access to ATN's official social media channels are limited to staff members who are designated the job of updating the social media channels. These staff members must not share the login details unless permitted by the e-Safety Lead.

7. Use of Personal Devices and Mobile Phones

- ATN recognises that personal communication via mobile technologies is an accepted and expected part of everyday life for staff, learners and those who access the services provided by ATN. However, these mobile technologies must be used safely and appropriately within ATN sites.
- All use of personal devices and mobile phones will take place in compliance with the law and other appropriate ATN polices, including, but not limited to: Anti- Bullying, Safeguarding and Data Protection
- Electronic devices that are bought onto site are the responsibility of the user at all times.
- Sending abusive or inappropriate messages/content via personal and mobile devices is forbidden by any staff member, learner and those who access the services provided by ATN. Any breaches of this will be dealt with by the e-Safety Lead.

7.1 Staff Use of Personal Devices and Mobile Phones

- Staff members will ensure that the use of personal devices and mobile phones will take place in accordance with the law and other appropriate ATN polices, including, but not limited to: Anti- Bullying, Safeguarding and Data Protection
- Staff members will be advised to keep their personal and mobile devices safe and secure at all times and not use these devices during lesson times.
- Staff members will not use personal devices, such as: mobile phones, tablets or cameras, to take photos or videos or learners without their expressed consent first. These photos or videos must only be used for official ATN purposes and never for personal use.
- If a member of staff breaches the e-Safety policy, action will be taken by the e-Safety Lead who will also record the incident.

7.2 Learner Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones. They will be made aware of boundaries and consequences of inappropriate use.
- ATN expects learners personal devices and mobile phones to not be used during lesson times
- Mobile phones and personal devices must not be used and should be concealed during examinations
- Learners will be advised to keep their personal and mobile devices safe and secure. ATN is not responsible for any loss or damage to personal and mobile devices, as the learner is held responsible for these items.

7.3 Visitors' Use of Personal Devices and Mobile Phones

- All visitors to ATN must use their personal devices and mobile phones in accordance with the law and other appropriate ATN polices, including, but not limited to: Anti- Bullying, Safeguarding and Data Protection
- All visitors are responsible for their own personal and mobile devices, as ATN is not responsible for any loss or damage to these items.

7.4 Officially provided mobile phones and devices

- Some staff members may be issued with a work phone and phone number. This must be kept safe and secure by the staff member at all times
- The usage of work phones will always be used in accordance with the law and other appropriate ATN policies, including, but not limited to: Anti- Bullying, Safeguarding and Data Protection

8. Responding to e-Safety Incidents and Concerns

- All ATN staff, learners and those who access the services provided by ATN will be made aware of the reporting procedure for e-Safety concerns, including: breaches of filtering, sexting, cyberbullying, fraud, downloading and using malicious software, masquerading and identity theft, illegal and inappropriate content.
- ATN requires staff, learners and those who access the services provided by ATN to work collectively to resolve e-Safety issues and concerns

- All ATN staff, learners and those who access the services provided by ATN must respect confidentiality and the need to correctly follow the ATN procedure for reporting concerns. All concerns regarding e-Safety must be reported to the e-Safety Lead.
- If there is suspicion that illegal activity has taken place, the e-Safety Lead will be immediately contacted or the Police will be called using 101, or 999 if there is an immediate danger or risk of harm

8.1 Concerns about Welfare of Learners

- The e-Safety Lead will be informed about e-Safety incidents involving safeguarding concerns. The Designated Safeguarding Team may also be informed.

Designation	Name	Telephone	Email
Managing Director of ATN and Safeguarding Lead	Sarjeet Singh Gill	02085749588	sgill@adult-training.org.uk
Regional Manager West London, Deputy Safeguarding Lead for London and North Hertfordshire	Kamaljit Kaur	02085749588	kamaljit@adult-training.org.uk
Community Engagement Officer and Deputy Safeguarding Lead for North Hertfordshire	Agnieszka Michalska	07885674321	agnieszka@adult-training.org.uk

- The e-Safety Lead will ensure that e-Safety concerns are appropriately dealt with and reported to the relevant agencies in line with the Safeguarding Vulnerable Adults procedures.

8.2 Staff Misuse

- Any complaint about staff misuse will be referred to the e-Safety Lead
- Any allegations regarding staff misuse or the online conduct of staff may result in an internal investigation
- Appropriate action will be taken in accordance with the policies of ATN

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Dealing with 'Sexting' and 'Revenge Porn'

- If ATN becomes aware of an incident regarding the creation or distribution of sexual imagery, ATN will:
    - Act in accordance with our Safeguarding policy
    - Immediately notify the Designated Safeguarding Lead
    - Carry out a risk assessment which considers the vulnerability of individual(s) involved
    - Make a referral to the Police if appropriate- when Section 33 of the Criminal Justice and Courts Act 2015 has been infringed
    - Provide necessary safeguards and support for the victim(s) involved, such as counselling or pastoral support
    - Implement appropriate sanctions in accordance with ATN's policies, but ensuring not to further traumatise the victim if possible
    - ATN will not view any sexual images that have been shared without consent, unless there is no other possible option, or there is a clear reason to do so. In this case, the image will only be viewed by the Designated Safeguarding Lead and the justification for viewing the image will be clearly documented.

9.2 Online Sexual Abuse and Exploitation

- ATN will ensure that all staff, learners and those who access the services provided by ATN are aware of online sexual abuse, including: exploitation and grooming; the consequences, the approaches that may be used by offenders and how to respond to concerns.
- ATN recognises online sexual abuse as a safeguarding issue and, as such, all concerns will be reported to the Designated Safeguarding Lead, who will respond accordingly.
- ATN will ensure that all staff, learners and those who access the services provided by ATN are made aware of the support available regarding online sexual abuse and exploitation.

9.3 Cyberbullying

- Cyberbullying, and other forms of bullying, will not be tolerated by ATN
- Full details on how ATN responds to cyberbullying are set out in the Safeguarding Policy- http://www.adult-training.org.uk/policies.html

9.4 Online Hate

- Online hate content, directed towards or posted by, ATN staff, learners or those who access the services provided by ATN will not be tolerated at ATN and will be responded to in line with existing ATN policies
- ATN staff, learners and those who access the services provided by ATN are advised to report online hate to the e-Safety Lead
- The Police will be contacted if a criminal offence is suspected and the Designated Safeguarding Lead will also be contacted

9.5 Online Radicalisation and Extremism

- ATN will take all reasonable precautions to ensure that all staff, learners and those who access the services provided by ATN are safe from terrorist and extremist material when accessing the internet on ATN premises. Full details are found in the ATN Safeguarding Policy, which incorporates ATN's Prevent Policy.
- If ATN becomes concerned about an individual who may be at risk of radicalisation online, the Designated Safeguarding Lead will be notified immediately and action will be taken in line with the Safeguarding Policy.

10. Useful e-Safety Links

→ https://safety.lovetoknow.com/Internet_Safety_Adult

→ http://www.bbc.co.uk/webwise

→ https://www.getsafeonline.org/protecting-yourself/

→ https://www.gov.uk/guidance/think-before-you-share

→ https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/

→ https://safe.met.police.uk/internet_safety/get_the_facts.html

→ https://safestars.org/internet-safety/

→ https://www.saferinternet.org.uk/

→ www.actionfraud.police.uk

Name: Sarjeet Singh Gill
Designation: Managing Director
Date: 15/05/19