




Norfolk Training Services

E-Safety and Acceptable Use Policy

Policy Reference		POL-0111 Version 1.0	
Author	Claire Charlwood	Date	29/06/2016
Approved By	William Wood		
Position	Chairman	Date	25/7/16
Review Cycle	Annually	Last Review	29/06/2016
Reviewed By		Review Due	June 2017

QLY-POL-pol-0111-v1.0-20160629

This policy contains 36 pages

Policy Document



Norfolk Training Services

Policies

What is a policy?

Policies provide a guiding framework for an organisation to conduct its business. These principles help to create behaviours, consistency and manage risks for our employees and the products and services we provide for learners, employers and partners.

The policy explains each principle, why it is needed, the activity required to support and uphold each principle, owners within NTS and the potential consequences if not followed;

Policies:

- Outline rules
- Provide principles that guide actions
- Set roles and responsibilities
- Reflect values and beliefs
- State an intention to do something

NTS policies are reviewed to ensure they are continually developed to take account of:

- Amendments to statutory requirements
- User and customer feedback
- New risks or conditions arising from new ventures or markets we operate in
- Audit results and recommendations
- External regulator/partner feedback and recommendations



Norfolk Training Services

Rationale

Norfolk Training Services (NTS) is committed to keeping all learners, other service users, and staff safe during their time at NTS.

The purpose of this policy is to ensure that all learners, service users and staff are kept safe (including any related personal information) while using NTS devices including computers, laptops, tablets, smart phones and mobile storage devices.

The policy outlines what NTS expects from staff, learners and other service users with regards to the 'acceptable use' of NTS ICT systems.

The policy also outlines what NTS considers acceptable use of the internet at home (given the internet is a global 24/7 communications tool) and the implications of breaches of this policy outside of working/learning time, including bringing NTS into disrepute through individuals' actions outside of the company.

This policy supports our wider '*Safeguarding children & vulnerable adults*' policy and our '*Preventing violent extremism*' policy and should be read in conjunction with these.



Norfolk Training Services

Legal and Other External Drivers

This policy pays due regard to the following legislation:

- Obscene Publications Act 1959 and 1964
- Public Order Act 1986
- Copyright, Design and Patents Act 1988
- Malicious Communications Act 1988
- The Computer Misuse Act 1990
- Protection from Harassment Act 1997
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Communications Act 2003
- Criminal Justice Act 2003
- Sexual Offences Act 2003
- Racial and Religious Hatred Act 2006
- Criminal Justice and Immigration Act 2008
- Defamation Act 2013



Norfolk Training Services

Framework and Principles

Definitions

E-safety

Web safety (or online safety or internet safety) can be described as maximising internet users' knowledge of the personal safety and security risks with regards to sharing private information online and self-protection from computer crime in general.

Acceptable Use

A set of rules applied by the owner of an ICT service that restricts how the ICT service may be used and sets guidelines for usage. This covers keeping personal data safe, professional and appropriate communications with service users and use of videos and other images of young or vulnerable people.

Personal data

This is defined in accordance with the Data Protection Act as data which relate to a living individual who can be identified (a) from those data or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the organisation.

Personal data also includes any expression of opinion about the individual and any indication of the intentions of the organisation or any other person in respect of the individual.



Norfolk Training Services

Framework and Principles

Acceptable Use Statement

NTS ICT systems are intended **only** for educational use by learners and for work-related purposes by staff. Learners and staff should be mindful that using NTS ICT systems for personal reasons may breach this policy.

At NTS, learners and staff are permitted to use the NTS ICT systems at their discretion as long as this **DOES NOT** involve:

- using the internet or email for the purposes of harassment or abuse
- using profanity, obscenities, or derogatory remarks in online communications
- accessing, downloading, sending or receiving any data (including images) which NTS considers offensive in any way, including sexually explicit or pornographic, discriminatory, defamatory or libellous material
- using the internet or email to make personal gains or conduct a personal business
- using the internet or email to gamble
- using the email systems in a way that could affect their reliability or effectiveness, for example, distributing chain letters or spam or downloading unsafe content.



Norfolk Training Services

Framework and Principles

Acceptable Use Statement (continued)

- placing any information on the internet that relates to NTS, altering any information about NTS and/or expressing any opinion about NTS unless specifically authorised to do so
- sending unprotected sensitive or confidential information internally or externally (including personal data)
- making official commitments through the internet or via email on behalf of NTS unless authorised to do so
- downloading copyrighted material such as music media files, film and video files (not an exhaustive list) without appropriate approval
- in any way infringing any copyright, database rights, trademarks or other intellectual property
- downloading any software from the internet without prior authorisation
- sharing images or videos of people under the age of 18 without their permission or the permission of their responsible parent/carer.



Norfolk Training Services

Framework and Principles

Acceptable Use Statement (continued)

- storing personal files such as music, video, photographs or games on NTS computers and devices
- removing or disabling anti-virus software or attempting to remove virus-infected files or clean up an infection, other than by the use of approved NTS anti-virus software and procedures



Norfolk Training Services

Framework and Principles

Acceptable Use Statement (continued)

In addition:

STAFF & LEARNERS should be mindful that they must not bring NTS into disrepute by posting offensive or defamatory comments on their personal social media accounts which may be accessed by members of the public who may link the content with NTS.

STAFF & LEARNERS should not seek to engage with each other via social media or communicate via messages (including text messages) UNLESS it is strictly for the purposes of education or work-related matters.

In the event that a member of staff has concerns about appropriate communication with a learner, they should seek advice from their **Manager** or the **Designated Safeguarding Lead** in the first instance before communicating with or responding to the learner.

In the event that a learner has concerns about appropriate communication with a member of staff, they should seek advice from the **Pastoral Support team** or the **Designated Safeguarding Lead** in the first instance before communicating with or responding to the staff member.



Norfolk Training Services

Framework and Principles

Acceptable Use Statement (continued)

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of personal data, NTS enforces a clear desk and screen policy as follows:

- Staff computers and other devices must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Staff must keep all NTS passwords and other NTS access codes strictly confidential and not share these with *anyone*, unless authorised to do so by a responsible Manager.
- Care must be taken not to leave confidential material (including personal data) unattended on desks, printers or photocopiers.
- All business-related printed matter (including personal data) must be disposed of confidentially or shredded.



Norfolk Training Services

Framework and Principles

Acceptable Use Statement (continued)

Working off-site

It is accepted that NTS laptops and mobile devices be taken off-site. In the event, the following controls must be applied:

- NTS laptops and other devices taken off-site must not be left unattended in public places and not left in sight in a car or other vehicle.
- Laptops must be carried as hand luggage when travelling.
- Information held on devices should be protected against loss or compromise when working remotely (for example, at home or in public places). Particular care should be taken with the use of laptops mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where they are used to access personal data relating to NTS, encryption.
- Staff are permitted to use personal mobile devices as long as they are authorised to do so by their Manager and have taken steps to ensure that any personal data relating to NTS is kept secure and that they do not breach the 'Acceptable Use' statement



Norfolk Training Services

Framework and Principles

Acceptable Use Statement (continued)

Mobile Storage Devices

- Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. These should always be encrypted to the company standard.
- Staff are permitted to use personal storage devices as long as they have taken steps to ensure that these do not breach the 'Acceptable Use' statement. These should not be used to store personal data relating to NTS.
- Staff should consult with a member of the MIS team about the secure transfer of personal data where they have any concerns.



Norfolk Training Services

Responsibilities - Corporate

As a training and service provider NTS will:

- maintain a visible and open safeguarding procedure in order that learners and staff can report concerns about unacceptable and/or abusive behaviour online
- communicate this procedure to all learners and staff from induction onwards
- ensure that all learners are adequately supervised while online at NTS or using NTS devices
- maintain a confidential and secure recording system for recording incidents, concerns and referrals.
- have a strategy in place for tackling cyber bullying and promoting e-safety.



Norfolk Training Services

Responsibilities - Corporate

As an employer, NTS will:

- ensure that staff working with young people and vulnerable adults are monitored and adequately supervised to minimise online risks to learners and themselves
- ensure that staff understand their personal responsibilities in relation to e-safety and the acceptable use of NTS and personal ICT
- provide staff with regular training and up-to-date guidance from induction onwards to ensure that they know how to recognise, respond to and report e-safety safeguarding concerns in accordance with their roles and responsibilities.
- take disciplinary action against any member of staff who breaches this policy or abuses a child, young person or vulnerable adult online.



Norfolk Training Services

Responsibilities – Directors

Directors

The Directors are responsible for ensuring that:

- this policy is acknowledged and respected by all, and as a result, that risks to the safety of all NTS online users are minimised
- they have an overview of safeguarding, including e-safety matters, at NTS to inform strategic decision-making with regards to the learning environment and that this work is appropriately prioritised and resourced to ensure it remains the highest priority
- all staff receive appropriate training and guidance with regards to E-safety and the 'Acceptable Use' statement.
- all devices accessible to learners are adequately risk assessed and the Directors are aware of the overall level of risk to NTS.



Norfolk Training Services

Responsibilities – Directors

Directors (continued)

The Directors are also responsible for ensuring that:

- personal data security is a principle which underpins all communications at NTS
- e-safety is promoted effectively throughout the organisation as part of the wider safeguarding agenda
- e-safety is monitored effectively as part of the wider safeguarding agenda
- accredited ISP/effective local filtering/parental controls on internet access are in place, as appropriate



Norfolk Training Services

Responsibilities – Managers

Managers

All Managers are responsible for ensuring that:

- their staff abide by this policy and have received appropriate regular briefings with regards e-safety and the 'Acceptable Use' statement
- they access training and guidance for their staff where they are concerned there may be the potential for breaches of this policy
- they monitor the internet usage by their staff through one-to-one supervision and spot checks
- any possible or actual breaches of this policy by staff, including the 'Acceptable Use' policy statement, are acted upon as a potential disciplinary matter and are reported immediately to the **Designated Safeguarding Lead** if a learner is placed at risk.



Norfolk Training Services

Responsibilities – Safeguarding

Designated Safeguarding Lead

- The Designated Safeguarding Lead will ensure that there is appropriate and up-to-date training and guidance available for all staff on e-safety and the 'Acceptable Use' statement as part of wider accredited safeguarding training.
- The Designated Safeguarding Lead will liaise with the Health & Safety Officer and with staff responsible for ICT to ensure that there is an appropriate risk assessment conducted on access to NTS devices.
- Where risks to learners are identified, the Designated Safeguarding Lead will respond to them in accordance with the '*Safeguarding children and vulnerable adults*' policy.



Norfolk Training Services

Responsibilities – Teaching & Support

Teaching & Support Staff

Teaching and support staff will ensure that:

- learners abide by the 'Acceptable Use' policy in the learning environment through monitoring and active supervision
- details of this policy are made available to all learners in the learning environment where learners have access to an NTS computer or other device
- they monitor the internet usage of their learners through one-to-one supervision and spot checks.
- any witnessed possible or actual breaches of this policy by learners (including the 'Acceptable Use' statement) are reported immediately to a **Manager** or the **Designated Safeguarding Lead** if a learner is at risk of harm.



Norfolk Training Services

Responsibilities – All Employees

All staff

All staff will ensure that:

- they are familiar with the contents of this policy and abide by this at all times, including the 'Acceptable Use' statement
- personal data (including their own) is kept safe, minimising the risk of loss or misuse
- they report any witnessed possible or actual breaches of this policy (including the 'Acceptable Use' statement by other staff or learners to a **Manager** or to the **Designated Safeguarding Lead** if a learner is at risk of harm



Norfolk Training Services

Responsibilities - Learners

Learners and other service users

Learners and other service users will:

- adhere to this policy (including the 'Acceptable Use' statement) at all times
- adhere to the relevant Code of Conduct with regards the use of personal mobile phones in the learning environment
- report any concerns that they have regarding the safe and appropriate use of the NTS computers or other devices to a member of staff
- not share their own or other people's personal information via the internet whilst at NTS

Impact of Not Adhering to Policy

The Telegraph, 2016

Kayleigh Haywood murder: Girl, 15, raped and killed after being groomed online and held prisoner, court hears



A 15-year-old girl was raped and murdered after fleeing partially-clothed from the home of a man who groomed her on Facebook, a jury heard.

Miss Moore said Kayleigh, from Measham, exchanged messages with Harlow on Facebook and went willingly to his home on November 13 after her telling her parents she was staying with her best friend.



Norfolk Training Services

Impact of Not Adhering to Policy

The Guardian, 2016

The internet's dangers were all too real for my son, Breck Bednar

Breck was groomed and murdered by a psychopathic, narcissistic paedophile he met in an online gaming forum. When I phoned the police two months before Breck's murder, the call handler and call closer failed to understand the signs of grooming, owing to either a lack of training or care.

Lorin LaFave (mother)



Impact of Not Adhering to Policy

The Guardian, 2013

A council has been fined £80,000 for losing the personal data of 286 children with special needs. The Information Commissioner's Office (ICO) served North East Lincolnshire council with the penalty after a memory stick went missing.

The unencrypted device contained sensitive information, including information about their mental and physical health problems and teaching requirements. It also included the pupils' dates of birth, some of their addresses and information about their home life.

The information has been missing since 1 July 2011, when the memory stick was left in a laptop at the council's offices by a special educational needs teacher. When the teacher returned to the laptop, the memory stick was gone and it has never been recovered, the ICO said.

Although the council had introduced a policy of encrypting portable devices in April 2011, it failed to make sure all of the memory sticks being used by staff were encrypted, the ICO said. The council was also unable to confirm if the teacher had received data protection training at the time of the loss.





Norfolk Training Services

Procedures

Checking and monitoring NTS computers and other devices

With regards to NTS computers and other devices accessed by **learners**, the following actions apply:

- Tutors and support staff will conduct regular spot checks of NTS devices (computers) used by learners, including browser and internet histories.
- Tutors will ensure that there is active supervision of learners whilst they are using NTS computers in the learning environment with the support of Learning Support Assistants. This will involve ensuring that there is always a member of staff present in the same room when learners are using computers and that learners are aware of this monitoring.
- Where Tutors or support staff have a legitimate concern about a learner's personal device (including any internet enabled smart phones, laptops or tablets), they may ask the learner to show them the content of the device. Any learner who fails to comply with a reasonable request to view content on a personal device may be subject to disciplinary proceedings or reported to the Police if there is concern of criminal activity.
- Where Tutors or support staff have a legitimate concern about criminal activity (e.g. distribution of illegal pornographic materials, or threatening behaviour) they may confiscate a learner's personal device and notify the Designated Safeguarding Lead who will report the matter immediately to the Police.



Norfolk Training Services

Procedures

Checking and monitoring NTS computers and other devices (continued)

With regards to NTS computers and other devices accessed by **staff**:

- Managers will conduct spot checks on staff devices at random intervals to ensure that their emails/browser/internet histories have appropriate content in accordance with the 'Acceptable Use' policy.
- Any member of staff may request that a manager check any NTS computer or device internet history where they have a legitimate concern of misuse.



Procedures

In the event of a breach or possible breach of the online safety policy or the unacceptable use of NTS devices, the following will apply:

- Any witnessed breaches of this policy or reported incidents of concern **involving a learner** will be recorded using a "*Record of Involvement*" form by the member of staff and passed to a member of the Designated Safeguarding Lead, as per the '*Safeguarding children and vulnerable adults*' procedures.
- All recorded incidents **involving learners** will be passed to the Designated Safeguarding Lead to log on the Safeguarding Log.
- Any incident where it is identified that there is a clear risk of harm to a learner (under age 18) will be passed to the Police and other appropriate authorities for advice and support. In these instances, learners and their parents/carers will be notified of this course of action by the Designated Safeguarding Lead.
- Any incident where it is identified that there is a possibility of criminal activity or the radicalisation of an individual, in accordance with the '*Preventing violent extremism*' policy, will be passed on to the Police and other appropriate authorities to handle by the Designated Safeguarding Lead. In such instances, learners and parents/carers do not have to be notified unless the Police confirm it is safe and appropriate to do so.



Incidents involving learners (continued)

- All recorded and logged incidents must be actioned before being closed.
- Incidents of harmful behaviour towards learners (including grooming, cyber bullying or attempts to radicalise learners) will be handled as a safeguarding incident and treated accordingly under the '*Safeguarding children and vulnerable adults*' policy.
- Incidents of learner misuse of the internet during learning or outside of the learning environment (e.g. cyber-bullying via social media), including any inappropriate or dangerous conduct online which may bring NTS into disrepute, will be treated as a disciplinary matter and will be investigated in accordance with the '*Behaviour Management*' policy.
- Where learners are found to be in breach of this policy including the 'Acceptable Use' policy statement, this will be considered a breach of the '*NTS Code of Conduct*' and may result in a learner being terminated from the programme.



Incidents involving staff

- Incidents of staff misuse of the internet during working time or outside of work (e.g. communication with current learners via social media), including any inappropriate or dangerous conduct online which may bring NTS into disrepute, will be treated as a disciplinary matter and investigated at the request of a manager in accordance with the staff 'Disciplinary Policy'.
- Where staff are found to be in breach of this policy (including the 'Acceptable Use' policy statement), this will be considered a disciplinary matter and may result in a dismissal.



Norfolk Training Services

Procedures

Use of images and videos of learners and other service users

- Learner's consent (and that of their parent/carer, if appropriate) for the taking, storing and using of digital images is obtained at the point of sign-up within the NTS training agreement and will be held on record for the duration of the course.
- Digital images are only used for specific work-related purposes such as the promotion of NTS or recording and celebrating the achievement of learners.
- Digital images will be destroyed when learners leave NTS unless they provide their express permission for these to remain on file for future use.



Norfolk Training Services

Risk Management

This policy will be audited on an annual basis or more frequently if there are changes to the relevant legislation.

Abidance by this policy will be monitored and measured through:

- 1) Monthly Safeguarding Team meeting (chaired by the Designated Safeguarding Lead and attended by all deputies and invited Managers. This meeting will include:
 - Review of ongoing e-safety safeguarding issues (including learner case files).
 - Any issues arising from the handling of disclosures and incidents.
 - The timeliness and robustness of which disclosures and incidents are handled.
- 2) Monthly safeguarding monitoring report (including e-safety) submitted to the Directors.
- 3) Annual audit of all processes and procedures relating to the safeguarding (including e-safety) of learners and employees.

Further Information

Advice and guidance for staff and learners

Staying Safe Online

- Do not post any personal information online – including address, email address or mobile number.
- Think carefully before posting pictures or videos of yourself. Once you have put a picture of yourself online most people can see it and may be able to download it - it is not just yours anymore.
- Keep your privacy settings on social media as high as possible.
- Never give out your passwords.
- Do not befriend people whom you do not know - staff and learners should not be in contact with each other via social media.
- Do not meet up with people you have met online. Speak to your parent or carer about people suggesting that you do.

Further Information

Advice and guidance for staff and learners

Staying Safe Online (continued)

- Remember that not everyone online is who they say they are.
- Think carefully about what you say before you post something online.
- Respect other people's views. Even if you do not agree with someone else's views, it does not mean that you need to be rude about them.
- If you see something online that makes you feel uncomfortable, unsafe or worried, leave the website, turn off your computer (if you want to) and tell a trusted adult (the NTS Designated Safeguarding Lead, manger, tutor or assessor during working hours) immediately.

Further Information

Resources

The National Crime Agency's "**Thinkuknow**" programme provides resources, training and support for professionals who work directly with children and young people. These are designed to help young people keep themselves safe from sexual abuse and exploitation by developing skills in identifying and avoiding risk, learning how best to protect themselves and their friends, and knowing how to get support and report abuse if they do encounter difficulties. All resources are downloadable for FREE once users have registered to the site.

<https://www.thinkuknow.co.uk/teachers/resources/>

BBC Bitesize – KS3 – ICT

"E-Safety" interactive game to spot the dangers online

http://www.bbc.co.uk/bitesize/ks3/ict/history_impact_ict/esafety/activity/

Further Information

Resources

UK Safer Internet Centre

The UK Safer Internet Centre delivers a wide range of activity to promote the safe and responsible use of technology by:

- operating an award-winning e-safety helpline for professionals working with children in the UK
- operating the UK's hotline for reporting online criminal content
- co-ordinating Safer Internet Day in the UK
- developing new educational and awareness raising resources for children, parents and carers and teachers to meet emerging trends in the fast-changing online environment.

<http://www.saferinternet.org.uk/advice-and-resources>

Further Information

For general enquiries about Norfolk Training Services' E-Safety and Acceptable Use policy and procedure please contact:

Gary Rose
Designated Safeguarding Lead/Learning Environment Manager
Norfolk Training Service Limited
Harford Centre
Hall Road
Norwich
Norfolk
NR4 6DG

Telephone 01603 259900 Ext #244

E-mail gary.rose@norfolktrainingservices.co.uk