E-Safety Policy

Definitions and Overview

This policy applies to all learners and particularly children, young people and adults who may need support and all staff, volunteers, partners and families living and working at Norton Webb, other external facilities, in the workplace or distance learning.

An e-Safety incident is considered to have occurred when a learner or staff member instigates, or is the victim of, an activity which utilizes Information and Communications Technologies (ICT) to endanger the personal safety, mental well being, or financial well being of another individual.

Activities which will be considered E-Safety incidents include, but are not limited to, the use of ICT to

- Access, view, copy or download illegal content, or materials, including, but not limited to:
  - Child pornography.
  - Materials inciting racial hatred or violence.
  - Materials that are deemed to be in connection with radicalisation or will place learners at risk of radicalisation.
- Access, view, copy or download inappropriate content, or materials, as defined by the Norton Webb's Acceptable Use of ICT policy.
- Bully or harass an individual or group (Cyber Bullying).
- Commit fraud or identify theft.
- Undertake any activities which would be in violation of the Child Protection, Protection of Vulnerable Adult or Anti-Bullying policies
- Any other incident where it can be reasonably considered that the personal safety, mental wellbeing or financial health of an individual has been endangered by the use of ICT.

In this context ICT includes, but is not limited to:

Norton Webb owned equipment, including:

- Desktop PCs
- Servers
- Laptop/Tablet devices
- Telephones, both fixed and mobile
- Digital video camera or camcorders
- Digital audio recording devices
- Reproduction devices (scanners, printers, etc..)
- Any and all software and IT services provided by the Norton Webb

Privately owned ICT equipment (including personal mobile phones), when:

- Connected to any Norton Webb owned network
- Utilised to access Norton Webb software and services

- Made use of on campus, or in the pursuit of Norton Webb business.

Legal Framework

Computer Misuse Act 1990

Makes provision for securing computer material against unauthorised access or modification; and for connected purposes.

Data Protection Act 2018/ General Data Protection Regulation (GDPR)

Makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Malicious Communication Act 1998

Makes provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety.

Counter-Terrorism and Security Act 2015

From 01 July 2015 all HE institutions, Norton Webb's, schools, and registered early years childcare providers are subject to a duty under section 26 of the act in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

The Education Act 2002 - Section 157 & 175

Requires local authorities and governing bodies of further education institutions to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children, young people and adults at risk. In addition they should have regard to any guidance issued by the Secretary of State in considering what arrangements they may need to make.

Working together to Safeguard children / young people (2015)

Provides statutory guidance on the roles and responsibilities of agencies working together to safeguard children/ young people. In addition it sets out the framework for the formation of Local Safeguarding Children Boards and details the allegation management process.

The Mental Capacity Act (2005)

Provides a way in which people who may need help to make decisions can get that help from someone who can be trusted to act in their best interests. Mental Capacity under the Act means being able to make your own decisions.

The Mental Capacity Act and its Code of Conduct contain a set of rules, procedures and guidance. The Act applies in full to those aged 18 or over, the entire Act except making Power of Attorney or Making a Will applies to 16 and 17 year olds. The Act only applies to those under 16 in very limited circumstances and these would have to be determined by a Court.

It is the responsibility of every staff member to give full and active support for the policy by ensuring:

- The policy is accessible, known, understood and implemented.
- All actual and suspected serious e-Safety incidents are reported to the safeguarding team.
- Parents/Guardians, providers, sponsors, employers and other stakeholders have a responsibility to report any e-Safety concerns they may have to the Norton Webb.
- All learners both Further and Higher education have a responsibility to:
  - Report any e-Safety concerns they may have to a member of staff, this could be a Progression Coach, Tutor or Learner Mentor.
  - Not engage at any time in any form of behaviour which would result in the occurrence of an e-Safety incident.

Reporting

All e-Safety incidents should be reported to a designated safeguarding person who will log the incident in the safeguarding database, and where necessary will engage with external agencies.

Securing and Preserving Evidence

IT Services should be contacted immediately following the reporting of any serious e-Safety incidents and asked to make copies of relevant access logs, files etc.

If it is believed that an immediate risk of exposure to illegal or inappropriate materials, or mental distress exists to staff or learners, the computer or devices should be turned off immediately. You should not 'shutdown' or log off as this may corrupt, delete or overwrite evidence, the power supply should be turned off at the wall or the battery should be physically removed.

The equipment should then be moved to a secure location.

Illegal Material or Activities

Where an e-safety incident is reported this matter will be dealt with very seriously. Norton Webb will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or to the Safeguarding Officer. Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the line manager will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally.

Depending on the seriousness of the incident, serious incidents will be dealt with by Senior Management, in consultation with appropriate external agencies.

The Head of IT Services is responsible for involving other senior managers and law enforcement agencies as required. IT Services will assume responsibility for obtaining, securing and preserving appropriate additional evidence. For example, remote screen shots, web filter logs etc.

If it is believed that there is a child protection issue the procedures outlined in the Safeguarding policy should be implemented.

Indecent imagery

It is a criminal offence to take, show, and share indecent images of children and young people, those under the age of 18 can face prosecution for taking indecent images of themselves and sharing them with others (Section 1 Protection of Children Act 1978).

Under no circumstances should any person make copies, including screen shots or print outs, of suspected child/ young person indecent imagery. Taking copies of such materials, even when intended for evidentiary purposes, is a crime.

Inappropriate Material or Activities

Inappropriate material or activities are considered to be any materials or activities which are considered as unacceptable by the Acceptable Use of IT policy.

Staff Access to Inappropriate Material

Where it is suspected that a staff member has been accessing inappropriate material, or attempting to access, the time and date of the incident should be noted and the concerns raised with the head of Human resources.

Learner Access to Inappropriate Material

Where it is suspected that a learner has been accessing inappropriate material, or attempting to access, the time and date of the incident should be noted and brought to the attention of the relevant Curriculum Leader or Head of Centr. The safeguarding team should be contacted who may then liaise with the IT Helpdesk to take copies of relevant access logs etc.

Cyber-Bullying

Cyber-Bullying can be defined as making use of IT to undertake to bully. Examples of cyber- bullying include, but are not limited to:

- Sending offensive or abusive e-mails, instant messages, or 'text' messages.

- Inviting selected individuals to chat room or website to discuss another individual who has not been invited.
- Posting offensive, defamatory or abusive messages about an individual or group to a public or members only internet forum.
- Using a digital camera to take humiliating images

Incidents of actual or suspected cyber-bullying should be dealt with in accordance with the Anti- Bullying policy.

Virus & Malware Protection

Norton Webb will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of Firewalls, servers, routers, work stations etc. to prevent accidental or malicious Access of systems and information. Digital communications, including email and Internet postings, over the Norton Webb network, will be monitored in line with the Network Usage Policy.

IT Services will make all reasonable efforts to ensure current, up to date, anti-virus and malware protection is installed on all Norton Webb systems. However, users of the systems have a responsibility to:

- Alert IT Services if they discover a fault with their anti-virus and anti-malware software
- Ensure personally assigned devices (i.e. laptops) are connected to the network at least once per month.

Norton Webb will provide mandatory training to all staff on e-Safety awareness and their responsibilities in the event of an e-Safely incident.

Document Control	
UKPRN	10018297
Published	5/7/2014
Responsibility	Managing Director
Last Revised	21/10/2020
Next Review	01/10/2021