KEY SKILLS TRAINING

E-Safety Policy

Management Team
Updated: December 2018
Ratified by Management Team: December 2018

Introduction

Key Skills Training e-safety policy aims to create an environment where pupils, staff, parents, governors and the wider Key Skills Training community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Through teaching ICT, we equip children and young people to participate in a rapidly changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information in a varied and stimulating way. ICT skills are a major factor in enabling them to be confident, creative and independent learners. As the aims of ICT are to equip children and young people with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible. We provide suitable learning opportunities for all young people by matching the challenge of the task to the ability and experience of the child.

Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all Key Skills Training stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this. Pupils, staff and all other users of Key Skills Training related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a list of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in Key Skills Training and at home; and ultimately beyond Key Skills Training and into the workplace.

Key Skills Training E-safety Policy Scope

The Key Skills Training e-safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider Key Skills Training community who use, have access to or maintain Key Skills Training and Key Skills Training related Internet, computer systems and mobile technologies internally and externally. The Key Skills Training will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the Key Skills Training site. 'In Loco Parentis' provision under the Children Act 1989 also allows the Key Skills Training to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The e-safety policy covers the use of:

- Key Skills Training based ICT systems and equipment
- Key Skills Training based intranet and networking

• Key Skills Training related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
• External access to internal Key Skills Training networking, such as webmail, network access, file-serving (document folders) and printing.
• Key Skills Training ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
• Pupil and staff personal ICT equipment when used in Key Skills Training and which makes use of Key Skills Training networking, file-serving or Internet facilities.
• Tablets, mobile phones, devices and laptops when used on the Key Skills Training site.

Managing Information Systems

Securely maintaining information

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and learners Local Area Network (LAN) security issues include:

• Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
• Users must take responsibility for their network use. For Link Key Skills Training staff, flouting electronic use policy is regarded as a reason for dismissal.
• Workstations should be secured against user mistakes and deliberate actions.
• Servers must be located securely and physical access restricted.
• The server operating system must be secured and kept up to date; through regular monthly patching
• Virus protection for the whole network must be installed and current.
• Access by wireless devices must be proactively managed and secured with WPA2 PSK (pre-shared key).

Wide Area Network (WAN) security issues include:

• Key Skills Training broadband firewalls are configured to prevent unauthorised access between Key Skills Training.
• Decisions on WAN security are made on a partnership between partner organisations.

Key Skills Training broadband network is protected by a cluster of high-performance firewalls at the Internet connecting nodes.

• The security of the Key Skills Training information systems and users will be reviewed regularly.
• Virus protection will be updated regularly.
• Personal data sent over the Internet or taken off site will be encrypted.
• Portable media may not be used unless it has been encrypted and virus checked.
• Unapproved software will not be allowed in work areas or attached to email.
• Files held on the network will be regularly checked.

• System capacity in relation to storage will be checked regularly.
• The use of user logins and passwords to access the network will be enforced.

Filter Management

• The Key Skills Training's broadband access provides filtering appropriate to the age and maturity of learners. There is flexibility in the filtering system to allow for changes in provision depending on the learning required.
• Any breaches in filtering should be reported to the ICT Support and/or emailed to the director of finance and premises at: staceytaylor@keyskillsnortheast.com
• If staff or learners discover unsuitable sites, the URL will be reported to the Data and assessment manager who will then record the incident and escalate the concern as appropriate.
• The Key Skills Training filtering system will block all sites on the Internet Watch Foundation (IWF) list.
• Changes to the Key Skills Training filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
• The Key Skills Training Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
• Any material that the Key Skills Training believes is illegal will be reported to appropriate agencies.
• The access strategy will be designed by educators to suit the age and curriculum requirements of the learners, with advice from network managers.

Monitoring the e-safety policy:

The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

• E-safety Coordinator/Officer
• Head of Education
• Designated Safeguarding Officer
• Teaching Staff
• External IT contractors

In the event of an e-safety incident, the following people will be informed within Key Skills Training (Key Skills Training e-safety Coordinator, Head of Education, Designated Person.)

E-safety policy review and evaluation schedule:

• The e-safety policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year. Additionally, the policy will be reviewed promptly upon:
• Serious and/or frequent breaches of the acceptable Internet use policy or other in the light of e-safety incidents.
• New guidance by government / LA / safeguarding authorities.
• Significant changes in technology as used by the Key Skills Training or pupils in the wider community.

• E-safety incidents in the community or local Key Skills Trainings which might impact on the Key Skills Training community.
• The e-safety policy review will be documented in the Key Skills Training development plan and Key Skills Training self-evaluation and improvement profiling.
• The Management Committee will receive a report on the progress, evaluation, impact and this report will include suitably redacted accounts and statistics of e-safety incidents and how these have been resolved, and counter measures implemented.

Key Skills Training Management and e-safety

• Key Skills Training senior leadership team is responsible for determining, evaluating and reviewing e- safety policies to encompass teaching and learning, use of Key Skills Training IT equipment and facilities by pupils, staff and visitors, and the agreed criteria for acceptable use by pupils, Key Skills Training staff and governors of Internet capable equipment for Key Skills Training related purposes or in situations which will impact on the reputation of the Key Skills Training, and/or on Key Skills Training premises.
• The e-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and Internet developments, current government guidance and Key Skills Training related e-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships.
• e-safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the Key Skills Training and wider Key Skills Training community.
• The leadership team is encouraged to be aspirational and innovative in developing strategies for e-safety provision.

The Key Skills Training e-safety Coordinator:

The Key Skills Training has a designated e-safety Coordinator who reports to the SLT and Governors and coordinates e-safety provision across the Key Skills Training and wider Key Skills Training community. The committee liaises with SLT, the Key Skills Trainings designated safeguarding officer and other senior managers as required.

• The Key Skills Training's e-safety coordinator chairs the Key Skills Training e-safety committee which includes representatives of the Key Skills Training SLT, teaching and support staff and governors.
• The Key Skills Training e-safety committee meets regularly.
• The Key Skills Training e-safety coordinator is responsible for e-safety issues on a day to day basis and also liaises with LA contacts, filtering and website providers and Key Skills Training ICT support.
• The Key Skills Training e-safety coordinator maintains a log of submitted e-safety reports and incidents.

• The Key Skills Training e-safety coordinator audits and assesses inset requirements for staff, and support staff e-safety training, and ensures that all staff are aware of their responsibilities and the Key Skills Training's e-safety procedures. The coordinator is also the first port of call for staff requiring advice on e-safety matters.
• Although all staff are responsible for upholding the Key Skills Training e-safety policy and safer Internet practice, the e-safety Coordinator, Heads of Key Skills Training and ICT support are responsible for monitoring Internet usage by pupils and staff, and on Key Skills Training machines, such as laptops, used off-site.
• The e-safety Coordinator is responsible for promoting best practice in e-safety within the wider Key Skills Training community, including providing and being a source of information for parents and partner stakeholders.
• The Key Skills Training e-safety coordinator (along with IT support) should be involved in any risk assessment of new technologies, services or software to analyse any potential risks

ICT support staff and external contractors:

• External ICT support staff and technicians are responsible for maintaining the Key Skills Training's networking, IT infrastructure and hardware. They are aware of current thinking and trends in IT security and ensure that the Key Skills Training system, particularly file-sharing and access to the Internet is secure. They further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
• Support staff maintain and enforce the Key Skills Training's password policy.

Teaching and teaching support staff:

• Teaching and teaching support staff need to ensure that they are aware of the current Key Skills Training e-safety policy, practices and associated procedures for reporting e-safety incidents.
• Teaching and teaching support staff will be provided with e-safety induction as part of the overall staff induction procedures.
• All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Agreement relevant to Internet and computer use in Key Skills Training.
• All staff need to follow the Key Skills Training's social media policy, in regard to external off-site use, personal use (mindful of not bringing the Key Skills Training into disrepute), possible contractual obligations, and conduct on Internet Key Skills Training messaging or communication platforms, for example email.
• All teaching staff need to rigorously monitor pupil Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the Key Skills Training site.
• Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.

• Be aware of online propaganda and help pupils with critical evaluation of online materials.
• Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Staff Use of Personal Devices

● Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
● Staff will be issued with a Key Skills Training phone where contact with learners or parents/carers is required.
● Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
● If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
● Staff should not use personal 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 the academy policy then disciplinary action may be taken. Designated Safeguarding Officer:
• The Designated Safeguarding Officer is trained in specific e-safety issues. Accredited training with reference to child protection issues has been accessed.
• The Designated Safeguarding Officer can differentiate which e-safety incidents are required to be
• reported to CEOP, local Police, LADO, Local Safeguarding Children's Board, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
• Possible scenarios might include:
    - Allegations against members of staff.
    - Computer crime – for example hacking of Key Skills Training systems.
    - Allegations or evidence of 'grooming'.
    - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.

• Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter, Instagram, Snapchat and Facebook to remove instances of illegal material or cyber bullying.

Pupils:

• Are required to use Key Skills Training Internet and computer systems in agreement with the terms specified in the Key Skills Training Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.

• Pupils need to be aware of how to report e-safety incidents in Key Skills Training, and how to use external reporting facilities, such as the Click CEOP button or Childline number.
• Pupils need to be aware that Key Skills Training Acceptable Use Policies cover all computer, Internet and mobile technology usage in Key Skills Training, including the use of personal items such as phones.
• Pupils need to be aware that their Internet use out of Key Skills Training on social networking sites such as Instagram is covered under the Acceptable Use Policy if it impacts on the Key Skills Training and/or its staff and pupils in terms of cyber bullying, reputation, or illegal activities.

Learners Use of Personal Devices

• 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 student's withdrawal from either that examination or all examinations.
• If a learner needs to contact his/her parents/carers they will be allowed to use a Key Skills Training phone. Parents/Carers are advised not to contact their child via their mobile phone during the Key Skills Training day, but to contact the Key Skills Training office.
• Children and young people should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Parents and Guardians:

• It is hoped that parents and guardians will support the Key Skills Training's stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at Key Skills Training and at home.
• The Key Skills Training expects parents and guardians to sign the Key Skills Training's Acceptable Use Agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to Key Skills Training systems such as extranets, websites, forums, social media, online reporting arrangement.
• The Key Skills Training will provide opportunities to educate parents with regard to e-safety through the Key Skills Training website.

Other users:

• External users with significant access to Key Skills Training systems including sensitive information or information held securely under the Data Protection Act should be DBS checked. This includes external contractors who might maintain the Key Skills Training domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

How will the Key Skills Training provide e-safety education?

Pupils – curriculum teaching: 'Teaching online safety in Key Skills Training (DfE, June 2019) outlines to Key Skills Trainings the importance of helping children and young people not only use the internet safely, but also give them opportunities to learn how to behave online. Throughout the new compulsory Relationships (Sex Education) and Health Education pupils will be taught what positive, healthy and respectful online relationships look like.

The PSHE curriculum will following the underpinning knowledge and behaviours:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

Throughout the curriculum teaching about potential harms will include:

- Age restrictions
- Content: How it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design which keeps 'users online for longer than they might have planned or desired'
- Privacy settings
- Targeting of online content
- Abuse (online)
- Challenges [to do something and post about it]
- Content which incites...hate, violence
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication
- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders

- E-safety is accessed as part of pastoral care – form time activities, assemblies, year group presentations, tutorial opportunities.
- E-safety events – such as Safer Internet Day and Anti Bullying Week.

Parents/Carers – information and events:

- E-safety information is directly available to parents via the Key Skills Training website and Key Skills Training which is update with the latest E safety news and issues.
- Key Skills Training subscribes to a dedicated E safety support platform. Key Skills Training will take advantage of occasions when there are large numbers of parents in Key Skills Training to promote e safety.

Staff – inset and training:

- E-safety information is directly delivered to staff via the IT Team
- A planned programme of e-safety training opportunities is available for staff, including on site inset, whole staff training, online training opportunities (for example E-safety Support courses), external CPD courses, accredited CPD courses, (for example CEOP) and Coordinator training.
- The e-safety Coordinator should be the first port of call for staff requiring e-safety advice.

ICT support staff – contractors, filtering and monitoring:

- IT support staff and contractors will ensure that bought in hardware and software solutions feature built in training provision
- Support staff and contractors will be DBS checked and agree and sign the Key Skills Training's e-safety.
- IT technical support staff and network managers have relevant industry experience and Microsoft/Cisco certified qualifications.

Policy guidance for handling personal data, dealing with freedom of information requests, and complying with privacy regulations pertaining to website data:

All of these areas are regulated by the Information Commissioner (ICO), and every UK organisation has to comply with the responsibilities and obligations as defined by the ICO. Key Skills Trainings are no different to any other organisation in this regard. The ICO guidance on how to comply with these obligations is updated regularly. Key Skills Training refer directly to this guidance in these areas.

When disposing of computer equipment, Key Skills Trainings needs to ensure all data, including personal data is wiped, not deleted from storage.

Use of IT facilities for curriculum teaching and learning:

Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested, Students should be trusted to be responsible when researching the Internet, and teaching staff will consider the age and maturity of the students.

General Data Data Protection and e-safety:

The GDPR sets out the key principles that all personal data must be processed in line with.

• Data must be: processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also stronger rights for individuals regarding their own data.

• The individual's rights include: to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all.
• The General Data Protection Act is relevant to e-safety since it impacts on the way in which personal information should be secured on Key Skills Training networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.
• Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the Key Skills Training population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network.
• Personal data should only be stored on secure devices. In other words, only computers, servers, file- servers, cloud space, or devices which require a username and password to access the information.
• Secure accounts need to be logged off after use to prevent unauthorised access.
• Personal e mails should not be used for Key Skills Training business.

Unsuitable / inappropriate activities - acceptable use

The Key Skills Training believes that the activities referred to in Appendix One would be inappropriate in a Key Skills Training context and that users should not engage in these activities in Key Skills Training or outside Key Skills Training when using Key Skills Training equipment or systems.

E-safety and the Law:

This e safety policy takes cognizance of the following legislation;

The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the Key Skills Training behaviour policy.)
Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998

General Data Protection Regulations Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988 Racial and Religious Hatred Act 2006 12
Protection of Children Act 1978
Sexual Offences Act 2003

Key Skills Trainings have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989, this enables Key Skills Trainings to remove personal information, cyber bullying and comments relating to Key Skills Training pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all Key Skills Trainings.

Useful links to external organisations:

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
EiS - ICT Support for Key Skills Trainings and ICT Security Advice: www.eiskent.co.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact local Police.
Sunderland Safeguarding Partnership: www.sunderland.gov.uk/safersunderland
Kidsmart: www.kidsmart.org.uk
Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix 1

Has the school an e-Safety Policy that complies with DfE guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. learners, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	Y/N
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, learners and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all learners (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all learners?	Y/N
Do parents/carers or learners sign an Acceptable Use Policy?	Y/N
Are staff, learners, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N

Is personal data collected, stored and used according to the principles of GDPR?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	Y/N