Your fastest way to learn. Why wait?

FIREBRAND

E Safety Policy

May 2018

Introduction

Firebrand recognises e-safety issues and the potential harm and risks it can pose to young people. All partner agencies, stakeholders, and educational settings and all other organisations within the community providing services to young people have a duty to understand e-safety issues as part of its wider safeguarding duties;

- Recognising their role in helping young people to remain safe online while also supporting staff
- Acknowledges that its role is strategic rather than operational as it is for partner agencies to develop and embed their own operational policies and procedures, and lines of accountability, in safeguarding young people when using Internet, Digital and Mobile Technologies (IDMT).
- This policy needs to be read in conjunction with the safeguarding policy and it is envisaged, that this document will provide a framework for partners in this regard in line with the following definition of e-safety.

The term e-safety is defined for the purposes of this document as the process of limiting the risks to young people when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection

Our vision is that all young people, staff and all those working with young people recognise the risks, dangers and potential harm that may arise from the use of Internet Digital and Mobile Technologies, that they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any e-safety concerns so that young people and staff are kept safe.

Background

Article 17 of the United Nations Convention on Rights of the Child (UNCRC) states that, "Young people have the right to get information that is important to their health and well-being. Governments should encourage mass media - radio, television, newspaper and internet content sources - to provide information that young people can understand and to not promote materials that could harm"
The Sexual Offences Act 20031 includes a number of offences related to child abuse online.
Firebrand is aware that the understanding and use of Internet, Digital and Mobile Technology (IDMT) is essential to helping and encouraging every young person to reach their full potential.
Firebrand has to raise awareness and educate those involved in young person's welfare and development about the dangers that young people can face in the online world, whilst accepting that safety in the online world is not the removal or banning of access to digital technologies in itself but rather education and training, for young persons and adults, around responsible use and potential dangers.
All organisations providing services for young people have a responsibility to ensure that they understand e-safety issues, know how to help everyone stay safe online and have procedures in place to support those working with young people in knowing how to respond when concerns arise.

Risks

Young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences. Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained.
The advantages of the internet can and should out-weigh the disadvantages.
However, we now have a greater understanding to the extent of the risks the digital world can pose to everyone.

Risks include:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse.

Contact

- Grooming using communication technologies to meet and groom young people with the intention of sexually abusing them (both on and off line exploitation).

Commerce/Conduct

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Forms of Abuse through Internet Digital and Mobile Technologies (IDMT)

- Young people have been ‘groomed’ online by adults (often pretending to be those who care) with the ultimate aim of exploiting them sexually.
- Young people have been bullied by other young people via social networking sites, websites, instant messaging and text messages; this is often known as ‘cyber-bullying’.
- Inappropriate (i.e. threatening, indecent or pornographic) images of children and young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people. This is a criminal offence under s45 of the Sexual Offences Act 2003.
- The dangers attached to gang culture can rapidly accelerate online as many gangs ‘advertise’ or promote themselves via websites or social networking sites or if threats of violence, threats to an individual’s life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites and images can easily be accessed online.
- Images of physical abuse, crime, racism, self-harm, terrorism or on physical violence to influence young minds.
- Ignoring the dangers that young people can face would lead to serious gaps in our responsibilities towards safeguarding and child protection.

Why do we need an e-safety policy?
Each new technology introduces new opportunities and challenges for young people, parents, carers and those working with young people. In order to minimise the risks involved from new technologies we need to understand how young people use IDMT and how this may be misused by those who may present a risk to young people. It is important that we know how to respond when concerns arise

In recent years the internet and other means of electronic communications have become increasingly accessible to young people. This provides great opportunities for young people in terms of education, information, communication and having fun. However, it also includes risks from those intent on sexually exploiting young people and from the inappropriate use of communications technology. This highlights the need to educate young people about the benefits, risks and responsibilities of using information technology. It also highlights the need to provide appropriate guidance to those working with young people.
Local Safeguarding Children Boards have an important role in co-coordinating and ensuring the effectiveness of local work to safeguard and promote the welfare of young people. This document aims to support organisations in reviewing their own e-safety agenda and to help in developing effective e-safety policies and procedures.

Stakeholders
Statutory and voluntary organisations that young people and families may use should consider having an e-safety policy. These include community groups and private sector organisations also.
This document aims to provide information for organisations in helping them to develop e-safety policies.

Objectives
All organisations that work with young people need to have an e-policy in place based on the following objectives:

1. **Ensuring** that all young people, parents/carers and foster carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world.
2. **Ensuring** that all people who work with young people have access to effective policies and procedures and effective training to safeguard young people at risk through online activity.
3. **Ensuring** that professionals know how to respond when concerns arise regarding the misuse of communications technology.

Objective 1: Ensuring that all young people, parents/carers and foster carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world.
As Internet Digital and Mobile Technologies are constantly changing there is information available to help young people stay safe on line, the following sites may help in developing an e safety policy:
www.thinkuknow.co.uk and www.ceop.co.uk

The Child Exploitation and Online protection (CEOP) centre delivers a multi-agency service dedicated to tackling and bringing offenders to account either directly or with local and international police forces and working with young people and parents to deliver their ThinkuKnow internet safety programme.
http://www.iwf.org.uk/

The Internet Watch Foundation was established in 1996 by UK internet industry to provide an internet hotline for public and IT
professionals to report potentially illegal online content with the intention of having the offending material removed.
www.pitda.co.uk

1.1 E-safety education

1. Young people need to be educated in the responsible and safe use of the Internet and other technologies through a range of strategies.
2. Organisations providing internet access to young people (schools, libraries, youth clubs etc.) must ensure that they do so in a way that is safe and age appropriate for young people by way of appropriate filtering systems etc.
3. Young people must be made aware that perpetrators who forward indecent images could be prosecuted under s45 of the Sexual Offences Act 2003 for the distribution of child pornography which may result in them being registered on the Sex Offenders Register if convicted.
4. Young people should be advised that not all information is true but can be misleading and derogatory.
5. Young people need to be made aware that they may encounter content on IDMT that distorts and misrepresents what constitutes a good and safe relationship.
6. Designated e-safety champions and leads should register with websites such as Ofcom in order to keep up to date with new digital technologies.

Websites:
www.ofcom.org.uk
www.ceop.gov.uk
www.thinkuknow.co.uk/parents

Objective 2: Ensuring that all people who work with young people have access to effective policies and procedures and effective training to safeguard those at risk through online activity
The Internet Digital and Mobile Technologies are constantly developing and evolving and this section is only intended to give an idea of the range of communications channels used by people to contact each other and exchange electronic data - including Child
abuse images.
Security is a complex matter and queries should always be referred directly to the responsible body relevant to the agency.
Employees and service users (including young people) should be aware that abuse of recognised policies and procedures could result in a withdrawal of technology provision and potential legal / disciplinary action being instigated against the perpetrator.

All users must be compliant to an Acceptable Use Policy (AUP) for example:

- Not act un-reasonably and be inconsiderate of other service users.
- Must take responsibility for their own network use
- Computer and internet access should have appropriate security and anti-virus protection.
- Must ensure to not disable or circumvent security measures – filters, encryption etc.

- Must not have personal and sensitive electronic data taken offsite without being security encrypted and authorised by management.
- Must not have unapproved software being introduced into local networks and not authorised by management.

2.1 Developing filtering standards

- It is important to use as a minimum an ISP who subscribes to the Internet Watch Foundation (IWF) filtering list. This will help to filter out some inappropriate content, but not all. Using an accredited Internet Service Provider (ISP) will also provide higher standards for filtering.
- Levels of internet access and supervision must be age appropriate and suitable for the young people.
- Filtering systems should be secure but adaptable.
- Professionals may sometimes require temporary access to a normally restricted website in order to carry out research for a project or study. Providing this can be justified by management, restrictions may be temporarily removed however access should be monitored.
- Access controls (filtering) fall into several overlapping types:
- Blocking strategies prevent access to a list of unsuitable sites.
- Maintenance of the blocking list is a major task as new sites appear every day.
- An “allow list” restricts access to a list of approved sites. Such lists inevitably limit young people’s access to a narrow range of information.
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- Management should ensure that regular checks are made to ensure that filtering methods selected are age appropriate, effective and reasonable.
- Access to inappropriate websites any material perceived to be illegal must be reported to management who should inform this to the appropriate agency.

2.2 Email

- Email is now an essential means of communication which can also be accessible via most mobile phones.
- A degree of responsibility has to sit with young people and professionals since as soon as email access is permitted it is very difficult to control.
- Restricting both incoming and outgoing email to specific addresses is possible, however, not always practical as addresses can easily be changed. Microsoft Office 365 mail used by most organisations is scanned and filtered for spam and has an editable abusive language filter.
- Email should not automatically be considered private and most organisations reserve the right to monitor email. However, there has to be a balance between maintaining the safety of young people and their rights to privacy, which are covered by legislation.
- Email content and tone must also be considered. Due to the impersonal nature of email, young people may write things or be aggressive or dismissive in tone which may be hurtful to others, even if such content or tone is not
- intended it may still be considered as cyber-bullying.
- Young people should also be encouraged to be creative and non-identifiable in setting up personal email addresses.

General guidance includes:

- Young people should not reveal personal information about themselves or other young people via email nor ever arrange to meet strangers by email without specific permission from an adult in authority and this should always be under supervision and preferably in a public place.
- Where possible, organisations such as education settings should consider the use of learning platforms and generic email accounts where students are required to submit coursework rather than by pupil to teacher's personal accounts.
- Organisations should always prohibit the forwarding of chain emails.
- Professionals should only communicate with young people by email if this has been agreed in advance with the child / young person, their parent/carer/foster carer and management and via equipment owned by their employer.
- It is a Professionals' responsibility if they have disclosed their personal email addresses to young people.
- Young people should advise a responsible adult or lead person if they receive offensive or threatening email.

2.3 Mobile Devices

Most young people now have access to mobile telephones which are generally perceived as essential to their day to day living and communicating and now offer access to the internet, instant messaging, email, social networking, a camera and video facilities. Mobile phones are becoming the most commonly used tool for internet access and social networking for young people. Mobile phones therefore pose one of the biggest online threats to young people as they allow instant access to all forms of IDMT.

- Young people and adults should be made aware to only share telephone numbers with those known to them and ensure that electronic records (call, text and email logs) are kept of any bullying or threatening telephone calls, text messages, emails or images received which may need to be used as evidence in any police investigation.
- Young people should be careful about accepting invitations to join location based social networking sites such as GyPSii that allow your location to be identified via GPS enabled phones.
- Settings may restrict the use of mobile devices during working hours.
- However, in some settings permitting responsible use of the mobile phone in conjunction with a cyber-bullying education programme is also an approach.

.

2.4 Social Networking

The Internet provides ready access to online spaces and social networking sites which allow individuals to publish un-moderated content. Social networking sites such as Facebook, Twitter, Chat Rooms, Online Gaming Platforms and Instant Messaging can connect individuals to groups of people which may be friends in the 'virtual' world but who may have never met each other in the real world. Users can be invited to join groups and leave comments over which there may be limited or no control.

Young people should be encouraged to consider the associated risks and dangers related to sending or accepting friend requests and posting personal comments, inappropriate images or videos about themselves or their peers and the subsequent
difficulty in removing an inappropriate image or information once published. They should also be advised not to publish detailed private thoughts or emotions which could be considered threatening, intimidating or hurtful to others.

Young people should also be encouraged to never give out any personal details or images which may identify themselves, their peers, their siblings / foster siblings, their location or any groups, schools or organisations they attend or associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos,IM and email addresses, including those of friends, family and peers. This also includes any 'gangs' they may be affiliated with.

Young people must be advised about e-security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others by making their profiles private and only accept friend requests from those already known to them. Care should be taken to delete old and unused profiles from websites which are no longer used as these will remain accessible to others. Personal information voluntarily shared by a young person is unlikely to remain the same as the person matures and has a greater understanding of how personal information about them can impact on their later lives (i.e. perspective employers making an online search of their name and sighting inappropriate photographs, videos or content etc.).

Professionals working or in a position of trust with young people (including volunteers) must also familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social networking sites with young people. They should be made aware that any inappropriate material posted could affect their professional status. Professionals must responsibly restrict access to their friends and family only and 'friend requests' by a young person may be within professional boundaries.
Professionals must also steer clear of social networking sites that young people are known to frequent except in certain roles.

2.5 Web Cam

It is now generally accepted that the term "child pornography" should not be used, because it conflates the images of child abuse (which constitute "child pornography") with adult pornography which may be perfectly legal. There are different opinions about this, but it has now become generally accepted that the term "child sexual abuse images" is more appropriate, and most agencies have adopted this practice in their written material. Individuals caught in possession of child abusive images will nearly always arise as a result of a police investigation and the seizure of images, possession of which is an offence under the Protection of Children Act 1978 – amended 1994. This states:

"It is an offence for a person….
a) …. to take, or permit to be taken, or to make, any indecent photographs or pseudo-photographs of a child
b) …. to distribute or show such indecent photographs or pseudo-photographs."

2.6 Multi-player games on line

Children, young people and responsible adults need to understand that their online behaviour may have consequences as although it's an online game the players are real people.

2.7 Cyber-bullying

Cyber-bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF 2007). young people should find using IDMT as a positive and creative part of their everyday life. Unfortunately, IDMT can also be used negatively to target a specific young person or group.

- It should also be noted that professionals, especially teachers and other education staff are particularly vulnerable to "cyberbullying" by young people, which may include general insults, threats, harassment, defamation, homophobic or racist remarks or other forms of prejudice based bullying. The effects of cyber bullying by young people on adults are equally distressing and the impact on the victim can be just as profound – Government guidance notes remind us that cyber bullying incidents are upsetting whoever the victim is and whatever age they are.
- Employers should be alert to the possibility and potential for cyber bullying towards members of staff by young people and appreciate there is no single solution to the problem.
- Instances of cyber-bullying must be responded to sensitively and in line with existing anti-bullying policies and procedures in the organisation.
- The victim of cyber-bullying must be reassured they have done the right thing in disclosing the bullying and be supported.

.

2.8 Publishing young people's images and work

- Many organisations create websites inspired by pieces of work and quotations and statements from young people. Often these can include images or videos of young service users which help promote and make the organisation identifiable to other young people.
- Still and moving images and sounds can add liveliness and interest to a publication, particularly when young people are included nevertheless the security of young people is paramount and names and identifiable locations of young people should never be linked to their images. (For example, a child placed in a refuge for domestic violence could be traced back to a school by their school uniform).
- Yonng people should also be advised when photographs or video footage of them is being taken and images should never be published without the consent of the young person, and the written consent of their parent/carer or foster carer.
- Although it is fairly simple to upload comments, images and videos on social networking and video broadcasting websites, young people must be encouraged to consider the associated consequential risks and dangers in doing this and the difficulties in removing this content, particularly if the content subsequently becomes the property of the publisher.
- Inappropriate offensive, pornographic or threatening content can have devastating consequences to individuals and groups (including gangs) and young people should be made aware of the legalities and long term implications of doing this.

2.9 Illegal Downloading

Whilst there are many sites where music, videos and software can be legally downloaded, young people and adults need to be made aware that they could be breaking the law by downloading copyright protected files or by infringing other intellectual property rights.

The various industries affected by illegal downloading (particularly music) do monitor the internet and can take legal action ranging from fines to suing those who hold parental responsibility. It is recommended that websites are thoroughly researched prior to downloading content for personal use.

Objective 3: Ensure that Professionals know how to respond when concerns arise regarding the misuse of communications technology.

3.1 e-safety complaints

▫▫Any complaints about e-safety concerns should be progressed via the organisations recognised complaints procedure which should be readily accessible to all; however efforts should be made to resolve low level issues internally.
These must be recorded locally.
▫▫All factors in relation to the complaint must be clearly established in order to have substance.
▫▫Complaints about employee's IDMT misuse should be escalated to the most senior manager within the organisation and be managed according to recognised disciplinary and child protection procedures.
▫▫Employers must have internal methods of scrutinising IDMT use, in particular, the ability to identify sites accessed. This is particularly important where there is an allegation that illegal or inappropriate websites have been accessed.
▫▫Potentially illegal issues must always be referred to the police in the first instance.

3.2 Monitoring e safety incidents and reporting abuse

Any form of electronic or digital abuse towards young people should in the first instance be reported to the Child Exploitation Online Protection service www.ceop.police.uk, and also reported to the relevant IDMT lead with the organisation. Any incidents which place a young person in immediate danger should be referred to the local police by calling 999.

Safeguarding Children Board seeks to ensure that partner agencies monitor the following as a suggested minimum dataset of e-
Safety incidents:

- A description of the e-safety incident
- Who was involved
- How the incident was identified
- What actions were taken and by whom
- Conclusions of the incident

3.3 Promoting the Policy

It is recommended that organisations include young people in the design and layout of their e-safety policy as their perceptions of risk will vary from age group to age group. Ideally, posters should be displayed in rooms where computers can be accessed which highlight the policy and reiterate that all network and internet usage will be monitored and appropriate action will be taken if abuse occurs. This policy should be made readily available to parents / carers and foster carers by way of being included and accessible on the
organisations published literature and website.

3.4 Staff Engagement

- All staff with responsibility for young people's learning via IDMT must be familiarised with this policy and given opportunities to raise issues and concerns they face in their day to day working responsibilities.
- All staff must understand that misuse of IDMT will result in disciplinary action being taken against them in line with your organisations policies and procedures.
- Employees unsure of what constitutes acceptable usage of the internet should always check with management. They should be aware that all internet usage is monitored and can be traced back to each individual user.
- Staff must also be aware of what is acceptable in terms of their engagement with young people via IDMT means
- Staff (including volunteers) should never disclose or share their personal details except in certain exceptional roles (i.e. personal mobile phone numbers, email

addresses or social networking profiles etc.) or send or accept friend requests on social networking websites with children and young people / service users.

Any necessary contact between a young person and a professional should be made via equipment and contact details provided by the employer (not personal equipment / contact details) and be clearly recorded on a need to communicate basis and with the consent of the parent/ carer or foster carer. Alternatively, personal contact details for children / young people should be stored centrally by management and only accessed on a need to know basis as approved by management.

- Organisations should adopt an open culture of vigilance in the workplace and staff must feel confident in identifying and challenging poor and/or risky working practices.
- Ideally, training on acceptable usage and responsible e-safety should be provided during the induction period for all new employees with a specific emphasis on professional boundaries, confidentiality and data protection.
- This section will help staff determine what action they can take when they identify concerns and should be read in conjunction with policy and procedures.

3.5 How do we respond?

The response required will depend on the nature of the incident. Concerns may relate to:

- The accidental access to inappropriate material
- Accidental access to illegal material
- Deliberate access to inappropriate material
- Inappropriate or illegal use of technologies
- Bullying or harassment using technology

Committing an Illegal Act - Did You Know?

- Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence.
- Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**
- Showing anyone else illegal material that you have received **is an illegal act**
- **Within 4 simple steps you couldeasily break the law 4 times. Each is a serious offence**
- Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it
- Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material
- Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material
- Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**
- **Never personally investigate.** If you open illegal content accidentally report it to your manager.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. Internet use and abuse is governed by many civil

or criminal laws in the UK. While this list is not exhaustive, some of the key provisions are summarised below:

- Computer Misuse Act 1990 (including hacking, denial of service attacks)
- http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

- Copyright, Designs and Patents Act 1988(including copyright theft)
- http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

- Crime and Disorder Act 1998
- http://www.opsi.gov.uk/acts/acts1998/19980037.htm

- GDPR

- https://www.eugdpr.org/

- Privacy and Electronic Communications (EC Directive) Regulations 2003(including spam)
- http://www.opsi.gov.uk/si/si2003/20032426.htm

- Protection from Harassment Act 1997 (including harassment, bullying, and cyber stalking)
- http://www.opsi.gov.uk/acts/acts1997/1997040.htm

- Protection of Children Act 1978, as amended by Section 84 of the Criminal Justice and Public Order Act 1994 (including indecent images of children)
- http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

- Malicious Communications Act 1988 (including harassment, bullying, and cyber stalking)
- http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

- Sexual Offences Act 2003 (including grooming)
- http://www.opsi.gov.uk/acts/acts2003/20030042.htm

The Obscene Publications Act 1959 and 1964 (including illegal material on, or transmitted via, the web and electronic communications) - not available online
The Telecommunications Act 1984 (including illegal material on, or transmitted via, the web and electronic communications) - Not available online

CYBERBULLYING & HARASSMENT

Cyberbullying can range from embarrassing or cruel online posts or digital pictures, to online threats, harassment, and negative comments, to stalking through emails, websites, social networks and text messages.

Every age group is vulnerable to cyberbullying, but teenagers and young adults are common victims. Cyberbullying is a growing problem in schools. Cyberbullying has become an issue because the Internet is fairly anonymous, which is appealing to bullies because

their intimidation is difficult to trace. Unfortunately, rumours, threats and photos can be disseminated on the Internet very quickly.

Protect Yourself from Cyberbullying:

- **Limit where your personal information:** Be careful who can access contact information or details about your interests, habits or employment to reduce your exposure to bullies that you do not know. This may limit your risk of becoming a victim and may make it easier to identify the bully if you are victimised.

- **Avoid escalating the situation:** Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. If you receive unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

- **Document cyberbullying:** Keep a record of any online activity (emails, web pages, social media posts, etc.), including relevant dates and times. Keep both an electronic version and a printed copy.

- **Report cyber bullying to the appropriate authorities:** If you are being harassed or threatened, report the activity to the local authorities. There is a distinction between free speech and punishable offenses. Police can help sort out legal implications. It may also be appropriate to report it to your facilitator who have separate policies for dealing with activity that involves safeguarding you and your information.

STOP. THINK. CONNECT.

- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's OK to limit how and with whom you share information.

- **Safer for me, more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

- **Post only about others as you have them post about you.** The Golden Rule applies online as well.

Authorisation & Document Control

Document Title	E Safety Policy			**Status**	V.2
Classification	External	**Last Review**	2018	**Next Review**	2019
Location	S:\Apprenticeship\Quality\Policies & Procedures\2017				

Authorisation	**Responsible Person or Body**
Document Owner	Barbara Turner
Authorised By	Kiely Makepeace

Version History

Version	Author	Issued	Summary of Changes
V.1	Barbara Turner	August 2017	Development of Policy & Procedure
V.2	Barbara Turner	May 2018	GDPR Updates