TILEYARD EDUCATION
E-SAFETY POLICY AND PROCEDURES
Policy Owner: Head of Student Services
Last Updated: December 2022
Last Reviewed: December 2022
Next Review Date: December 2023

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

CONTENTS 2

AIM AND SCOPE

TILEYARD EDUCATION (TYE) E-Safety policy and procedures apply to all staff, contractors, tutors, volunteers, trustees, children, young people and anyone working on behalf of TYE.

The aim of the policy is to:

- Protect children and young people who receive TYE's services and who make use of information and communication technology (such as mobile phones, games consoles and the internet) as part of their involvement with TYE.
- Provide staff and volunteers with the principles that guide TYE's approach to E-Safety.
- Protect professionals.
- Ensure that, as an organisation, TYE operate in line with our values and within the law in terms of how we use information technology.

This E-Safety Policy is to be read in conjunction with TYE's Safeguarding and Child Protection Policy.

TYE recognises that the welfare of the children/young people who come into contact with our services is paramount and governs our approach to the use and management of information and communication technologies (ICT).

TYE will promote E-Safety by:

- Appointing an E-Safety Coordinator – Harry Leckstein
- Having procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT.
- Supporting and encouraging the children and young people using our service to use the opportunities offered by mobile phone technology and the internet in a way that keeps them safe and shows respect for others.
- Educating and providing information for parents on e-safety.
- Supporting and encouraging parents and carers to keep their children safe online and when using their computers, mobile phones and game consoles.
- Incorporating statements about safe and appropriate ICT use into the codes of conduct for staff and volunteers and for children and young people.
- Having an e-safety agreement with children and young people.
- Using our procedures to deal with any inappropriate ICT use, complaints and/or allegations by anyone working for or using TYE's services.
- Informing parents and carers of incidents of concern as appropriate.
- Regularly reviewing and updating the security of our information systems.
- In the event of a suspected breach of E-Safety, the E-Safety coordinator to investigate.
- Ensuring that images of children, young people and families are only used after their written permission has been obtained from their parents or guardians, and only for the purpose for which consent has been given.

TYE will handle complaints regarding E-Safety by taking all reasonable precautions to ensure E-Safety and giving staff/volunteers, contractors and children/young people information about infringements in use and possible sanctions.

Sanctions include:

- Interview with a member of staff or contractor
- Informing parents/carers
- Removal of mobile phone, internet or computer access for an agreed period of time
- Referral to local authority/police

The E-Safety coordinator Harry Leckstein will be the first point of contact for any complaint. Any complaint about staff/volunteer's misuse will be referred to the relevant E-Safety lead and may result in formal disciplinary proceedings. Any complaint about the E-Safety coordinator will be referred to the Company Secretary and may result in formal disciplinary proceedings.

If the relevant E-Safety Coordinator is not available, the complaint to be referred to the Chair of Trustees. Complaints of cyber-bullying are dealt with in accordance with TYE's Behaviour and Safeguarding and Child Protection Policies.

Concerns related to child protection are dealt with in accordance with the London Safeguarding Children Board's child protection procedures at www.islingtonscb.org.uk

E-SAFETY OFFICER

Harry Leckstein (harry@tileyard.co.uk / tel +44 (0)7796 950 406)

The responsibility of this role is to:

- Develop an E-Safety culture.
- Be the named points of contact on all E-Safety issues.
- Monitor E-Safety.
- Ensure that everyone: staff/volunteers, children/young people, management committee members and Trustees know what to do if they are concerned about an E-Safety issue.
- Keep abreast of developing E-Safety issues via http://www.islingtonscb.org.uk/key-practice-guidance/Pages/E-Safety.aspx
- Ensure that E-Safety is embedded within continuing professional development (CPD)for staff/volunteers.
- Co-ordinate training as appropriate.
- Ensure that E-Safety is embedded across all activities as appropriate.

● Ensure that E-Safety is promoted to parents/carers, other users and children/young people.
● Ensuring that the infrastructure and technology provide a safe and secure environment for children/young people.
● Maintain an E-Safety incident log to record incidents and concerns.
● Monitor and report on E-Safety issues to the management team and management committee.
● Review and update E-Safety policies and procedures on a regular basis and after an incident.

RISKS AND ISSUES

The following are the range of technologies children/young people and staff/volunteers use positively but which can also put them at risk:

● Internet
● E-mail
● Instant messaging Blogs
● Podcasts
● Social networking sites
● Chat rooms
● Gaming Sites
● Mobile phones with camera and video functionality
● Mobile technology (eg games consoles) that are internet ready and include webcams
● E-smart phones with e-mail, web functionality, camera and video functionality and secure text network

Risks can come under the categories outlined below:

	Commercial	Aggressive	Sexual	Values
Content That the user may come across either accidentally or via a deliberate search	Adverts Spam Sponsorship Requests for personal information Exposure to age inappropriate material	Violent/hateful content	Exposure to illegal material, eg, images of child abuse Pornographic/ unwelcome sexual content	Bias Racist Misleading information/ advice

Contact Unsuitable contact from another user	Tracking Harvesting Publishing information about themselves	Being bullied, harassed, stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct	Illegal downloading Gambling	Bullying or harassing another	Creating and uploading inappropriate/	Providing misleading
User's behaviour that creates risk either through illegal activity or lack of awareness of the potential consequences	Hacking Financial scams		abusive material 'Sexting'	information/ advice

VULNERABILITY OF CERTAIN GROUPS

Some groups of children are more vulnerable to being abused through the use of technology and are less resilient to deal with it. Technology can also increase their offline vulnerability. These children need further protection to keep them safe.

These groups of children include:

● Looked After Children. There is evidence that children who are looked after and children who are adopted are using social networking sites to access their birth families, and birth families are using social networking sites to contact their children, even though there may be a court order prohibiting any contact. This results in unmediated contact.

● Children with disabilities. Studies have shown that pupils with Special Educational Needs are 16% more likely to be persistently cyber bullied over a prolonged period of time. These children may be more socially naïve.
● Children living away from their families can make them more vulnerable, for example, children living in residential units, boarding school, privately fostered.
● Children at risk of sexual exploitation. Technology is used to contact, groom and control these children. Research states that it has been rare to identify cases of child sexual exploitation where the use of technology has not been a factor. For more information about children at risk of sexual exploitation refer to ISCB's website: http://www.islingtonscb.org.uk/key-practiceguidance/Pages/Sexual-Exploitation.aspx .
● There is general risk to adolescent girls with the proliferation of websites aimed at them that promote anorexia, related eating disorders and 'starving for perfection'.
● There is general risk to boys who can be at high risk of addiction to violent games and pornography.

CYBERBULLYING

What is cyberbullying?

Cyberbullying is the use of technology such as mobile phone, internet, e-mail, social networking sites, chat rooms and instant messaging services to deliberately upset someone else.
● It can be used to carry out all the different types of bullying, an extension of face-to-face bullying.
● It can also go further, by invading home/personal space and can involve a greater number of people.
● It is an anonymous method by which bullies can torment their victims at any time of day or night.
● It can draw bystanders into being accessories.
● It includes: threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images; and manipulation.
● It includes sexting, sending explicit images electronically. These images can be widely distributed
● It also includes trolling, the online posting of inflammatory messages with the intention of provoking an emotional response. This can involve violent threats, poking fun, making trouble and causing annoyance.
● It can involve setting up hate websites or groups on social networking sites.
● It can take place across age groups and adults working with children can be targeted, for example, by pupils and/or parents.

Impact on the victim

The victim may receive email, chat, text messages or posts on social networking sites that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Cyberbullying can pose a serious threat to their physical and emotional safety.

Responding to cyberbullying

TYE will address all incidents of bullying thoroughly and sensitively.Victims of cyber bullying will be offered the immediate opportunity to discuss the matter with a member of staff who will reassure the child and offer support. They will be reassured that what they say will be taken seriously and handled sympathetically.

Staff will support the individual who has been cyber bullied. Keeping them under close supervision and checking their welfare regularly. Children who have been perpetrators of cyber-bullying will be helped by discussing what has happened, establishing why the child became involved. Staff will help the child to understand why this form of behavior is unacceptable and will encourage him/her to change their behavior.

If the cyber-bullying behavior persists, more serious actions may have to be taken which may involve consultation with parents and suspension or exclusion.

In all cases of cyberbullying TYEwill ensure that the evidence is preserved.

TYE will respond as follows to cases of cyberbullying:

- Change or if not possible encourage the victim to change their mobile phone number.
- Report the bullying to the site where it was posted.
- Try to get content removed from the web.
- Investigate the possibility of the victim blocking the person bullying from their sites and services.
- Ask the person bullying to delete the offending content and say who they have sent it on to.
- Contact the police in cases of actual/suspected illegal content.
- Consider the bystanders who can amount to hundreds of young people.

ACCEPTABLE USE POLICY (AUP)

TYE's AUP clearly identifies the expectations and boundaries for the use of technology both provided by TYE and those provided by individuals for their personal use.

AUP applies to the use of computers, laptops, mobile phones, smart phones, cameras and video cameras, webcams, games consoles and other technology that may be available within the organisation.

TYE Staff/volunteers and users should be aware of the potential consequences of any breach of the AUP.

TYE will deliver/access e-safety awareness raising and training for staff/volunteers and users.

For the workforce - staff/volunteers:

● Induction of new staff/volunteers will include information on E-Safety and the associated policies.

● TYE staff/volunteers will receive training that includes how to differentiate between their personal and professional behaviour especially when they are online.
● TYE will develop appropriate strategies for the safe and responsible use of technology as part of the workforce's everyday practice.
● All staff/volunteers must sign an AUP contract.
● Monitor your workforce's internet use if possible.
● Report any issues that arise as a result of monitoring to TYE's named E-Safety persons.

For children/young people:

● Include children/young people in developing E-Safety policies where possible.
● Children/young people that use TYE's ICT must sign an AUP contract.

For parents and carers:

Raise parents/carers' awareness of E-Safety through training, where appropriate, and displaying/distributing information.

7. FORM A – STAFF / VOLUNTEERS ACCEPTABLE USE POLICY

This agreement covers the use of digital technologies in TYE including email, internet, intranet, network resources, software, equipment and systems.

I will only use TYE's digital technology resources and systems for professional purposes.

I will not reveal my password(s) to anyone.

I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.

I will not use anyone else's password if they reveal it to me and will advise them to change it.

I will not allow unauthorised individuals to access any TYE systems.

I will ensure all documents, data, etc are saved, accessed and deleted in accordance with TYE's network and data security and confidentiality protocols.

I will not engage in any online activity that compromises my professional responsibilities.

My personal online communication tools, including mobile phones, will not be used with service users and I will not communicate or 'befriend' any service user using these methods.

I will only use the approved email system for any email communication related to work at TYE.

I will not browse, download or send material that could be considered offensive to colleagues and users.

I will report any accidental access to or receipt of inappropriate materials, or filtering breach to the responsible E-Safety coordinator Harry Leckstein.

I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.

I will not publish or distribute work that is protected by copyright.

I will not connect a computer, laptop or other device (including USB flash drive) to the computers/internet that does not have up-to-date anti-virus software.

I will not use personal digital cameras or camera phones for taking and transferring images of children/young people or staff/volunteers without written permission and will not store images at home.

I will ensure that any private social networking sites/blogs, etc that I create or actively contribute to are separate from my professional role.

It is my responsibility to ensure that my use of social networking sites/blogs, etc does not compromise my professional role, eg, setting appropriate security settings.

Any computer or laptop loaned to me TYE is provided solely for professional use

I will access TYE's resources remotely (such as from home) only through approved methods and follow E-Security protocols to access and interact with those materials.

Any confidential data that I transport from one location to another will be protected by encryption.

I will follow TYE's data security protocols when using confidential data at any location.

Any information seen by me with regard to service users held within TYE will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

It is my duty to support a whole organisation safeguarding approach and I will alert the named Safeguarding/Child Protection officer or Chair if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern.

I will not use, access or set up a Facebook or any other social networking site to follow a child's/parent's/carer's movements or activities. I will not monitor or investigate their social networking sites. If I come across a child's/parent's/carer's social networking account or site I will not enter it. If I have Safeguarding/Child .

Protection concerns about a child's/young person's behaviour on-line, or if I think social media could provide critical information, for example, if a child is missing or is at risk of harm, I will contact the police and children's social care.

It is my responsibility to ensure that I remain up-to-date, read and understand TYE's most recent E-Safety policies.

I understand that all internet/network usage can be logged and this information can be made available to my manager on request.

I understand that failure to comply with this agreement could lead to disciplinary action

I agree to abide by this agreement.

Signature ..... Date .....

Full Name ..... (printed)

Job title ..... Authorised Signature

I approve this user to be set-up.

Signature ..... Date ..... Full Name ..... (printed)

Job title .....

FORM B – CHILDREN AND YOUNG PEOPLE'S ACCEPTABLE USE AGREEMENTS B.1 FOR PEOPLE OF 13 OR OVER

This agreement covers the use of digital technologies in TYE including email, internet and equipment ("ICT").

I will use TYE's ICT systems in a responsible way, to ensure that there is no risk to my safety, the safety of others or to the safety and security of the ICT systems.

TYE may monitor my use of the ICT systems, email and other digital communications.

I will not share my password nor will I try to use any other person's username and password.

I will not disclose or share personal information about myself or others when on-line.

If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. I will report this to the Youth Worker in Charge or if unavailable to the E-Safety Co-ordinator Harry Leckstein or Trustee responsible for E-Safety

I will not use TYE's ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

I will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

I will not use strong, aggressive or inappropriate language when I communicate with others.

I will not take or distribute images of anyone without their permission.

If I use my own devices (Mobile phone) in TYE I will follow the rules set out in this agreement, in the same way as if I was using TYE's equipment.

I will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others.

I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to these materials.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email because of the risk of the attachment containing viruses or other harmful programmes.

I will not install or attempt to install programmes of any type on any equipment or store programmes in a computer.

I will not try to alter computer settings.

I will only use chat and social networking sites with permission and at the times that are allowed.

Where work is protected by copyright, I will not try to download copies, including music and videos.

I have read and understand the above and agree to follow these guidelines.

FULL NAME……(printed)

Signature ..... Date .....

FORM C: E-SAFETY INCIDENT MONITORING FORM

Details of person completing the form Name: Phone number: Email:
Date of incident:
Where did the incident take place?
Names of those involved in the incident:
Age(s) of child(ren) involved:
Was the incident? Child on Child Child on Adult Adult on Child Adult on Adult
Type of incident Sexual Grooming Bullying Violence Hate/incitement Financial Other Please give details:
What media was used? Social networking BBM or other free system MSN Email Webcam Mobile Phone Games Console Other Please specify:
What action was taken in relation to those involved in the incident? Please give details:

What follow-up action was taken?

Referral to LADO Referral to Children's Social Care Advice to parents Police investigation

Other

Please give details:

FORM D: E-SAFETY TRAINING RECORDS

NAME	COURSE	DATE	MANAGER'S SIGNATURE

Tileyard Education Limited, (09959654)
Lynton House, 7-12 Tavistock Square
London WC1H 9LT

APPENDIX 1 - E-SAFETY TIPS FOR ADULTS WORKING WITH CHILDREN AND YOUNG PEOPLE

Set your privacy setting to “Just Friends” so that your details, photographs, location, etc can only be seen by your invited friends.

Have a neutral picture of yourself as your profile image.

Don't post potentially embarrassing material.

Reject or ignore friendship requests unless you know the person or want to accept them.

Choose your social networking friends carefully and ask about their privacy controls.

Do not accept ‘friendship requests’ on social networking or messaging sites from children/young people (or their parents) that you work with.

For groups and networks set your privacy setting to private or everyone in the group or network will be able to see your profile.

If you wish to set up a social networking site for a work project create a new user profile for this. Do not use your own profile.

Use location settings wisely. Many social networking and online applications disclose your location. Where this is specifically linked to your identity it will, within a couple of days have disclosed where you live and when you are not at home.

There are social networking groups to bring together people sharing experiences, such as attending festivals and conferences. This advertises when you will not be at home.

Be careful not to leave your Facebook account logged-in in a shared area/household. Someone could leave status messages that may compromise or embarrass you. This is called Frape (Facebook Rape) and can be a form of cyber bullying.

If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name

Think before you post. Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a “web crawler” and it will always be there.

Be aware of addictive behaviour. Adults are just as likely as young people to get hooked on social networking, searching or games.

When you log-into a web site, unless your computer is exclusive to you, do not tick boxes that say 'remember me'.

Do not leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.

Use strong passwords that include a mixture of upper and lower case letters, numbers and other characters, are a minimum of 8 characters in length and do not contain the person's username. Do not to use the 'Remember Password' feature of applications.

Turn Bluetooth off when you are not using it. If you open un-pass worded Bluetooth anyone with Bluetooth in range can read the content of your phone or device.

Lock your mobile. Set a pin number or password for your mobile phone. With access to email, social networking and contacts an unlocked mobile phone can put your identity, and others, at risk.

APPENDIX 2 - PARENTS' / CARERS' INFORMATION

E-safety is concerned with safeguarding children in the early years age range in the digital world. It is about learning to understand and use new technologies and Information Communication Technology in a positive way. E-Safety is not about restricting children, but educating them about the risks as well as the benefits so they can feel confident and happy online.

To keep your children safer online:

- Know what your child is doing online much like you would offline.
- Make an effort to get computer literate if you want to support and understand your children, you need to have a reasonable understanding of their world.
- Talk to your child. Share the experience with them and ask them to show you how they use technology.
- Be open and encourage them to talk to you.
- Establish how the internet will be used in your house.
- Agree the type of content that you would be happy for them to download, knowingl receive or send on to others.
- Discuss what will be kept private online, eg, information, bank and credit card details and photos.
- Encourage balanced use – switching off at mealtimes, bedtime.
- Use a child friendly search engine.
- Install antivirus software, filtering and firewalls.
- Secure your internet connections.
- Use parental control functions for computers, mobile phones and games consoles.
- Remember that tools are not always 100% effective and sometimes things can get past them. Locate the computer/laptop in a family room and don't allow webcams to be used unless with your consent and always in a family room under supervision.
- Encourage your child not to hesitate about coming to you about anything they see online which upsets or disturbs them.
- If your child reports a problem make sure you support them, report it or seek advice.
- Save any abusive messages or inappropriate images for evidence purposes.
- Be aware of how to report nuisance calls or texts.

APPENDIX 3 - USEFUL CONTACTS/WEBSITES

Katy Potts – for advice on E-safety training and policy implementation katy.potts@islington.gov.uk

Websites

BBC Learning zone www.bbc.co.uk/learningzone/clips/5594.flv
Child Exploitation and Online Protection Centre (CEOP) http://ceop.police.uk/
Childnet International http://www.childnet-int.org
Cyberbullying www.digizen.org
Cybermentors https://cybermentors.org.uk/
Get Safe Online http://www.getsafeonline.org/
Information Commissioner's Officer
http://ico.org.uk/for_organisations/data_protection/
Islington Safeguarding Children Board – E-safety
page http://www.islingtonscb.org.uk/key-practice guidance/Pages/E-safety.aspx
Internet Watch Foundation To report indecent content http://www.iwf.org.uk/
Kidsmart http://www.kidsmart.org.uk/
KnowItAll (KIA) www.childnet-int/kia)
Ofsted http://www.ofsted.gov.uk/resources/safe-use-of new-technologies
Safe network http://www.safenetwork.org.uk/Pages/default.aspx
ThinkuKnow (TUK) www.thinkuknow.co.uk

APPENDIX 4 - GLOSSARY OF TERMS

Age related filtering	Differentiated access to online content dependent on age and appropriate need
AUP	Acceptable Use(r) Policy
Blogging & social networking	Anyone can produce and distribute their own content and link with other sites to create a very powerful network for sharing ideas and influence opinion
CEOP	Child Exploitation and Online Protection centre
Cyber bullying	Bullying using technology such as computers and mobile phones
Downloading	Receiving information or data electronically usually through the internet; this could include saving a document, picture, music or video from a website
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device
E-safety	Limiting risks to children/young people when using Information and Communications Technology (ICT). E-safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT: fixed or mobile, current, emerging and future ICT
Filtering	Software that can help to block a lot of inappropriate material but they are not 100% effective
Firewall	A buffer between your computer and the internet. It limits incoming and outgoing information, and keeps your computer safe from intruders. It can't stop you downloading spyware, but it can alert you if a program is sending information over the internet without your permission
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, Nintendo DS

Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'
Hacking	When your details, online accounts or other personal information is accessed by a stranger

ICT	Information and Communications Technology, eg, mobile phones, gaming consoles, computers, email, social networking
Identity Theft	When your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud or deception
ISP	Internet Service Provider. A company that connects computers to the internet for a fee
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide
Locked down system	In a locked down system almost every website has to be unbarred before it can be used. Only vetted websites can be accessed
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses)
Managed system	In a managed system the organisation has some control over access to websites and ideally offers age-appropriate filtering
Password - strong	A strong password contains a mixture of upper and lower case letters, Numbers and other characters. It is recommended to be a minimum of 8 characters in length

Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen
Profile	Personal information held by the user on a social networking site
RUP	Responsible Use(r) Policy
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal, sexual images or conversations to another party, usually via mobile phone or instant messaging
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process)
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people

Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email)
Spyware & adware	A general term for malicious software that is designed to take control of a computer without the consent of the user. Adware is one type of spyware - computer programs in which commercial advertisements are automatically shown to the user without their consent
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers
Trolling	Posting inflammatory messages with the intention of provoking an emotional response

Uploading	Sending and saving information or data from a local system, eg, mobile phone or computer, to a remote system, eg, a website
URL	Universal Resource Locator or website address
VOIP	Voice Over Internet Protocol
Youtube	Social networking site where users can upload, publish and share videos