Connaught School for Girls

ICT and E-Safety Policy 2019

Consultation Date: Curriculum Leaders : May 2019

Curriculum Sub Committee : June 2019

Date of Ratification by the Governing Body: July 2019

Review Date: July 2022

ICT and E-Safety Policy

E-Safety education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing (ICT) / PHSE / other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and form time/ pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the student Acceptable Use Agreement (AUP) and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/ Carers evenings / 'time4us' sessions at least 1 per academic year
- High profile events and campaigns such as Safer Internet Day
- Reference to the relevant websites / publications/ LGfL parents resources eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/ network is as safe and secure as is possible and that policies and procedures approved within this policy are implemented.

The school uses LGfL(London Grid for Learning) as its broadband connection provider, which is secured and filtered by the latest WebScreen 3.0 Firewall Filtering system.

The filtering policies consist of a combination of the following items which are defined as either blocked or allowed:

- website categories
- URLs and IP addresses
- keywords

All websites are placed into categories by the filtering engine. When someone surfs to a website, the system checks the category of the website and the policy being used to see whether access should be granted or not.

Within the school, all users of the network (wired and wireless), whether staff or student, using school provided access will need to use their network credentials (after agreeing to the Acceptable Use Policy) to access any internet or network content.
This provides the user an appropriate level of filtering within the system (either staff level or student level) as well as creating a live audit trail of a user's or device's internet use and browsing history.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems carried out by the network manager.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices through AUP agreements.
- All users at ks3 and ks4 will be provided with a username and secure password for the school network where it is still used, and for a Google area to access their Drive. Users are responsible for the security of their username and password and will be required to change their password regularly.
- The "administrator" passwords for The school ICT system, used by the Network Manager (or other person) must also be available to the SLT lead for ICT or other nominated senior leader and kept in a secure place.
- The SLT member for ICT and the network manager are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced/ differentiated user-level filtering that is consistent across all school devices.
- An appropriate system is in place for users to report any actual/ potential technical incident/ security breach to the network manager helpdesk, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- On request, the provision of temporary access of "guests" (trainee teachers, supply teachers) onto the school systems can be made.
- An agreed policy is in place (see AUP documents) for use of school systems.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/ carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act or under GDPR policy). To respect everyone's privacy and in some cases protection, these images should not be published/ made publicly available on social networking sites, nor should parents/ carers comment on any activities involving other students in the digital/ video images.
- Staff and volunteers are allowed to take digital/ video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes and images must only be kept in accordance with the GDPR retention schedule.
- Care should be taken when taking digital/ video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images and within guidance on GDPR regulations.
- Students' full names will not be used anywhere on a website or blog in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (this is covered as part of the AUP signed by parents or carers at the start of school- see Parents / Carers Acceptable Use Agreement)

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks/ disadvantages.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored through school system filtering. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report, to a member of staff – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/ carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

This school has a duty of care to provide a safe learning environment for students and staff. The school could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, students' parents/ carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

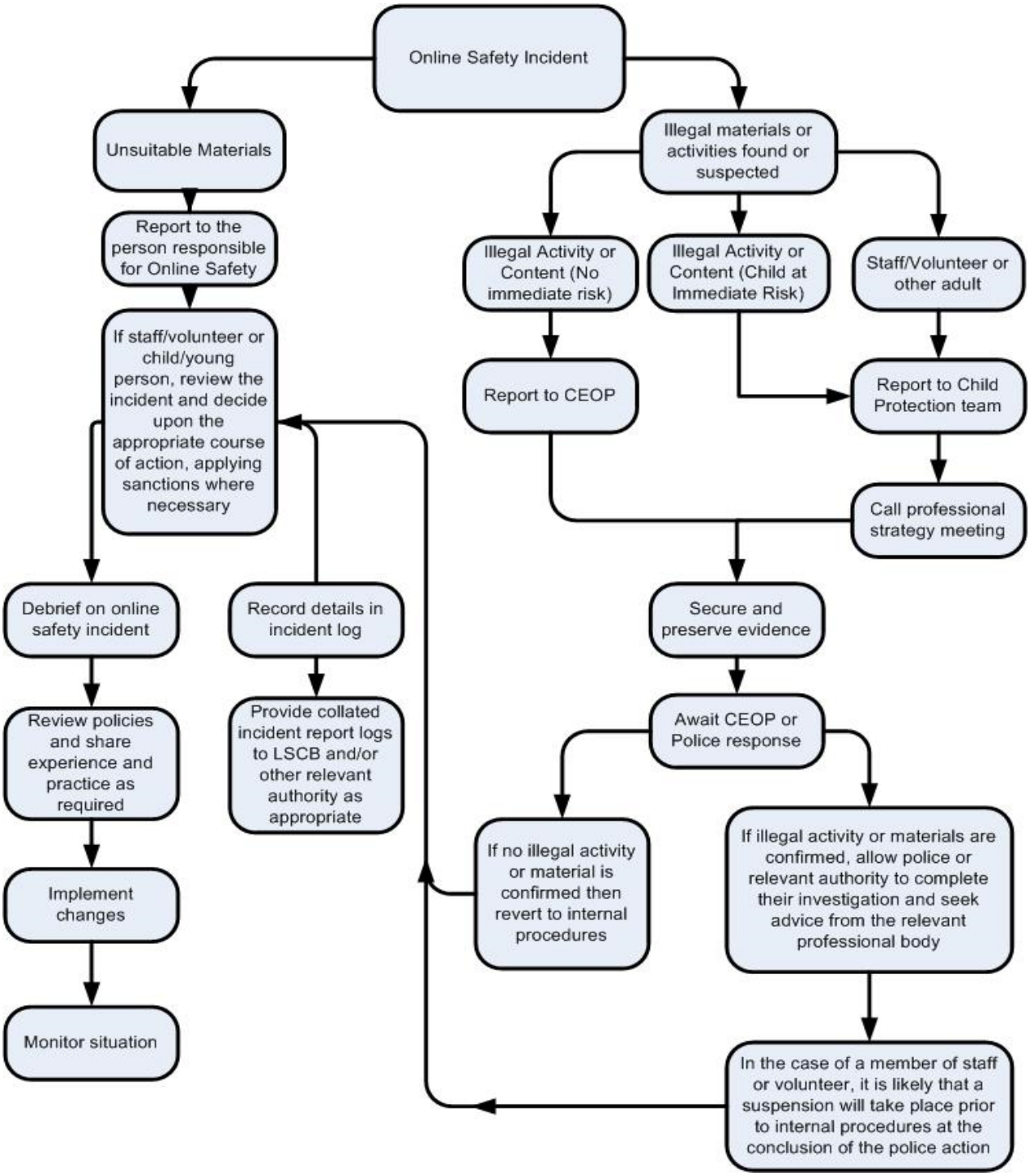
The school's use of social media for professional purposes will be checked regularly by SLT lead for ICT to ensure that it best represents the corporate image of the school.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above)

Illegal Incidents

If there is any suspicion that the web site concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, an investigation through this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/ local organisation (as relevant).
    - Police involvement and/ or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour.
    - the sending of obscene materials to a child.
    - adult material which potentially breaches the Obscene Publications Act.
    - criminally racist material.
    - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

School Actions & Sanctions

Poor student behaviour should be challenged as per the schools behaviour policy, and in the first instance should always be dealt with by class teachers.

Category A infringements:

- Use of non-educational sites during lessons.
- Unauthorised use of email.
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends.
- Use of unauthorised instant messaging/ social networking sites.

Sanctions: referred to class teacher.

Category B infringements

- Continued use of non-educational sites during lessons after being warned.
- Continued unauthorised use of email after being warned.
- Continued unauthorised use of mobile phone (or other new technologies) after being warned.
- Continued use of unauthorised instant messaging/ chatrooms, social networking sites, NewsGroups.
- Accidentally corrupting or destroying others' data without notifying a member of staff of it.
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it.

Sanctions: referred to Class teacher, Assistant Head (ICT)/ removal of Internet access rights for a period/ contact with parent.

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others.
- Sending an email or social network message that is regarded as harassment or of a bullying nature (one-off).
- Deliberately trying to access offensive or pornographic material.
- Any purchasing or ordering of items over the Internet.
- Transmission of commercial or advertising material.

Sanctions: as category B and referred to Assistant Head (ICT and/ or Safeguarding), HoY involved/ Parents contacted for meeting.

Other Safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site.
2. Inform service provider.
3. Inform Police (if appropriate)

Category D infringements

- Continued sending of emails or other messages regarded as harassment or of a bullying nature after being warned.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998
- Bringing the school name into disrepute

Sanctions – Referred to safeguarding lead/ Head Teacher/ Contact with parents/ possible exclusion /removal of equipment /refer to Community Police Officer

Other safeguarding actions

1. Secure and preserve any evidence.
2. Inform Police (if appropriate).

16 Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network/ use of VPN to mask illicit behaviour.

Sanction - referred to line manager/ Headteacher/ Warning given/ further sanction if necessary for gross misconduct

Category B infringements (Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of GDPR regulations.
- Significant breaching of copyright or license e.g. installing software key generation software on network/ use of VPN to mask illicit behaviour.
- Bringing the school name into disrepute.

Sanction - referred to Headteacher for disciplinary action.

Social Media

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/ carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Social Media Appendix

Managing your personal use of Social Media:

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Don’t use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts:

The Do’s

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school’s reporting process
- Consider turning off tagging people in images where possible

The Don’ts

- Don’t make comments, post content or link to materials that will bring the school into disrepute
- Don’t publish confidential or commercially sensitive material
- Don’t breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
- Don’t post derogatory, defamatory, offensive, harassing or discriminatory content
- Don’t use social media to air internal grievances

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document

CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
VPN	Virtual Private Network - Used to bypass security firewalls and mask the users behaviour and actions on the internet and school network.