Clifton High School
co-educational nursery pre-school to sixth form

Policy applies from EYFS to Sixth Form	**E-Safety**
Date policy updated	01.09.2019
Date Policy to be reviewed	01.08.2020 or earlier to reflect any changes in legislation
Author	Ms A Taylor Designated Safeguarding Lead (DSL) Contact details ataylor@cliftonhigh.co.uk
Designated Safeguarding Lead Support (DSLS)	Miss C Mulholland, Early Years Foundation Stage (EYFS) Contact details cmulholland@cliftonhigh.co.uk Mrs H Tabb, Year 3 – 6 Contact details htabb@cliftonhigh.co.uk Ms N Widdison, Year 7 – 11 Contact details nwiddison@cliftonhigh.co.uk Mr S Adams, Year 12 and 13 Contact details sadamds@cliftonhigh.co.uk
Deputy Head with responsibility for Child Protection and Safeguarding	Dr M Caddy Contact details mcaddy@cliftonhigh.co.uk
Designated Members of Council with responsibility for Child Protection and Safeguarding	Mrs H Vaughan Contact details hvaughan@cliftonhigh.co.uk Mrs J Morrison Contact details jmorrison@cliftonhigh.co.uk

Clifton High School is committed to child protection and safeguarding children and young people and expects all staff, visitors and volunteers to share this commitment.

Related Documents
Child Protection and Safeguarding
Data Protection, Retention and Management
Misconduct and Discipline
Online Filtering and Monitoring
School Rules
Staff Acceptable use of ICT Agreement
Staff Code of Conduct
Taking, Storing and using Photographs or Video (Parents)
Taking, Storing and using Photographs or Video (Staff)

At Clifton High School it is understood that Information and Communication Technology (ICT) provides a very important part of the pupils learning experience and that they exist in an online world. It is understood that due to the ever-changing nature of online environment, it is not possible to always be specific about new threats – it is the underlying intention that matters most.

The aim at Clifton High School is to promote the positive use of ICT and ensure that all pupils, all parents and all those working with pupils recognise the risks and potential dangers that may arise from the use of Internet, Digital and Mobile Technologies (IDMTs), 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 pupils are kept safe. The term “e-safety” is specifically defined for the purposes of this document as the process of limiting the risks to pupils and staff when using IDMT through a combined approach to policies and procedures, education and training.

The main areas of risk for our school community are

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content
- Grooming
- Cyberbullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
- Privacy issues, including disclosure of personal information or publishing of images/video without consent
- Digital footprint and online reputation
- Health and well-being (amount of time spent online)
- Sexting (sending and receiving of personally intimate images)
- Copyright (little care or consideration for intellectual property and ownership)

Roles and Responsibilities

Governors and Head of School

- Take overall responsibility for e-safety
- Ensures that staff receive suitable training to carry out their e-safety roles
- Ensure that the Clifton High School is an environment in which pupils can learn and staff can work safely whilst using IDMT
- Are aware of the procedures to be followed in the event of a serious e-safety incident

Staff

- Must follow the Clifton High School Acceptable use of ICT Agreement
- Must follow the Clifton High School policy on Taking, Storing and using Photographs or Video. Refer to Taking, Storing and using Photographs or Video (Staff)
- Must abide by the Staff Code of Conduct. Refer to Staff Code of Conduct
- Must abide by the Clifton High School style guide for email communication in the staff area of the Clifton High School website
- Should embed e-safety issues in all aspects of the curriculum and other school activities
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). Pupils are taught basic work place computer etiquette in Computing
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- Are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies regarding these devices
- Report any suspected misuse or problem to the Class Teacher, Tutor, Assistant to the Deputy Head, DSL or DSLS
- Must be aware of current e-safety issues and guidance e.g. through Continued Professional Development (CPD)
- Model safe, responsible and professional behaviours in their own use of technology
- Ensure that any digital communications with pupils is on a professional level and only through school-based systems, never through personal mechanisms, e.g. personal email, text, mobile phones, social networking

Parents

- Must follow the Clifton High School policy on Taking, Storing and using Photographs or Video (Parents). Refer to Taking, Storing and using Photographs or Video (Parents)

- Are kept informed of any new issues that may affect pupil safety and which may affect the wider school community. This is done through the Clifton High School Parents bulletin, which is emailed to parents weekly and information evenings organised through the school
- Consult with the school if they have any concerns about their children's use of technology
- Read, understand and promote the pupils' Contract of Behaviour Code and School Rules with, for the purposes of this policy, reference to the rules for safer internet use

Pupils

- Must abide by the rules for the safe use of the internet
    - Email and internet access are a privilege and not a right, and is provided to assist pupils with their work and to help them improve their IT skills
    - Pupils are responsible for the content of any email which is sent from their account. Pupils who act inconsiderately or irresponsibly or abuse the system may have its use withdrawn and a more serious consequence
    - Pupils should be aware that all their school electronic communications could be subject to scrutiny
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Follow the school policy on the taking/use of images and videos
- Know and understand the school policy on cyberbullying
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Know and understand the school policy on the use of mobile phones and hand-held devices.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Look after each other, and to report any concerns about the misuse of technology, or worrying issues to a member of staff, who will take appropriate action
- Know that sanctions for the misuse or attempted misuse of the internet, mobile phones and other electronic devices will be imposed
- Treat staff and each other online with the same standards of consideration and good manners as they would during face to face contact

Education and Training

Pupils receive e-safety guidance throughout the school curriculum but through Computing lessons, circle time, PSHE, Life Skills and assemblies. They are taught to

- Understand acceptable behaviour when using an online environment/email,
- Understand why they should not post or share detailed personal information and to know how to ensure they have turned-on privacy settings
- Understand why they must not post pictures or videos of others without their permission
- To know not to download any files without permission and have strategies for dealing with receipt of inappropriate materials
- Be aware that child sexual exploitation can occur using technology
- Be aware of the possible forms of online sexual harassment
- Be aware that radicalisation can occur through social media and the internet
- Know how to seek help if they experience problems when using the internet and related technologies and how to report any form of online abuse

Members of staff are updated regularly on e-safety issues through professional development and staff meetings and new members of staff are provided with information and guidance as part of the induction process.

Keeping the School Network Safe
The IT Manager is responsible for ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack and that the school meets the e-safety technical requirements. For more information see the Online Filtering and Monitoring Policy.

Network Security
- There is tight lock down of user rights and account security
- All users are required to change their password in every 12 months using strong password requirements
- Users have access only to certain limited areas they are authorised to use
- No software installation is possible without the approval of IT Services Department

A modern Unified Threat Management (UTM) device called SmoothWall is used in front of the network as a shield. It provides Internet content filtering, a powerful reporting suite, real time activity monitoring, social media controls, real time instant messaging word/phrase search generating alerts, firewall functions and VPN connectivity. Both LAN and Wi-Fi connected devices are monitored.

Additionally, the school has procured Impero Software to filter websites for students that are not considered of educational value. The latest version of Impero provides an updated keyword library filtering pornography, racial, cyberbullying, radicalisation and other violent content and detects common terms. These lists are automatically updated with each new Impero version.

Email Antivirus and Spam protection
Clifton High School uses an industry grade protection in Microsoft Office 365 with built in mal-ware and spam capabilities that help protect inbound and outbound messages from malicious software and spam. The IT manager can provide further granular control and customisation through the Exchange Admin Centre.

General Antivirus Protection
Sophos Antivirus protects every desktop PC or laptop we use in school. This offers a centralised control, install and clean-up facility in case of virus breakout.

Filtering
SmoothWall offers a built-in Internet content filtering solution. It uses a predefined list of various categories that Clifton High School can manually alter.

Wi-Fi network
The Wi-Fi network is totally separated from the domain network. It has been configured to use a Virtual Lan network (VLan), which provides Internet access for Clifton High School users using their personal login. The same rules apply for Wi-Fi users as well as desktop users and the Internet content filtering offers good protection.

Monitoring
During supervised teaching and learning the pupils will only be able to access internet sites through the filtered Clifton High School internet system, whether using their own mobile devices or the school computers. All computers on the school network are monitored through Impero. The IT Manager has access to the Impero Event Log, which records all Applications, Websites visited and violations.

As most pupils are using 3G and 4G on their personal devices whilst at school, pupils are required to access only sites available to them through the filtered Clifton High School Internet system. The use of the Internet is monitored and members of staff are instructed to question pupils seen using their mobile devices outside of lesson time to ensure correct use. Random monitoring of email is also in

place. Any issues with content will be forwarded to the relevant member of Senior Leadership. A record of searches and outcomes will be kept securely in the IT department.

Taking, Storing and Using Photographs or Video
Photographs and videos are regularly taken for recording a pupil or group of pupils participating in activities or celebrating their achievements and are an effective form of recording their progression (especially in EYFS). It is essential, that photographs or video are taken and stored appropriately to safeguard all pupils. Refer to Taking, Storing and using Photographs or Video (Staff) and Taking, Storing and using Photographs or Video (Parents). Members of staff are not permitted to use their own devices for taking photographs. EYFS staff members are prohibited from having their own devices in the classroom.

Mobile Phone Use
Refer to the Misconduct and Discipline Policy, School Rules, Staff Acceptable use if ICT Agreement Staff Acceptable use of ICT Agreement and Taking, Storing and using Photographs or Video (Staff)

Specific Safeguarding Issues
Cyberbullying

- Cyberbullying can be a form of peer-on-peer abuse. The Anti-Bullying Policy describes the preventative measures and the procedures that will be followed when cases of cyberbullying are identified
- Proper supervision of pupils plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe online. Pupils are taught of the possible consequences of cyberbullying and what to do if it happens to them
- Staff must follow the Staff Acceptable use if ICT Agreement to stay safe
- Harassment and bullying by pupils online will not be tolerated

Preventing Radicalisation
Children are vulnerable to extremist ideology and radicalisation. This can occur through many different methods including social media and gaming.

Online Sexual Harassment
This may be stand/alone or part of a wider pattern of sexual harassment and /or sexual violence. It may include

- Non-consensual sharing of sexual images and videos
- Sexualised online bullying
- Unwanted sexual comments and messages, including, on social media
- Sexual exploitation: coercion or threats

Child sexual exploitation is a form of child sexual abuse, which can occur through the use of technology. This is when an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of the perpetrator or facilitator.

Sexting is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the Internet. Pupils may also call it cybersex or sending a nudie, picture or selfie. Sexting is illegal. By sending an explicit image, a pupil is producing and distributing child abuse images and risks being prosecuted, even if the picture is taken and shared with their permission. It is easy to send a photo or message but the sender has no control about how it's passed on. When images are stored or shared online they become public. They can be deleted on social media or may only last a few seconds on apps like Snapchat, but images can still be saved or copied by others. These images may never be completely removed and could be found in the future, for example when applying for jobs or university.
Pupils may think 'sexting' is harmless but it can leave them vulnerable to

- Blackmail when an offender may threaten to share the pictures with the pupil's family and friends unless the pupil sends money or more images
- Bullying may result when images are shared with their peers or in school
- Unwanted attention when images posted online attract the attention of sex offenders, who know how to search for, collect and modify images
- Emotional distress resulting from embarrassment and humiliation. If they are very distressed this could lead to suicide or self-harm

Pupils are informed of the consequences of sexting and the legal implications through PSHE and assemblies.

Responding to incidents of misuse

It is expected that all members of the school community will be responsible users of ICT, however, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential to report it to the Assistant to the Deputy Head and IT Manger as soon as possible and it will be dealt with through normal behaviour/disciplinary procedures. If a child protection or safeguarding issue arises then the Child Protection and Safeguarding Policy must be followed. If any apparent or actual misuse appears to involve illegal activity the school will follow http://www.swgfl.org.uk/staying-safe guidance. If cyberbullying has taken place the Anti Bullying Policy will be followed.

Sources of Further information

http://www.swgfl.org.uk/staying-safe
www.childnet.com
www.Thinkuknow.co.uk
www.o2.co.uk/nspcc
www.ceop.police.uk