WHITGIFT SUMMER SCHOOL

ONLINE SAFETY POLICY

Introduction

Whitgift embraces advances in technology, especially when used to support learning. While the internet and social media are exciting, there is a need to address the dangers and raise awareness of potential abuses of that technology. In the light of recent high-profile cases in the media, such as instances of sexual grooming via chat-rooms, and strong evidence of online strategies being employed to radicalise young people, parents might understandably be concerned about a number of internet-related threats to the welfare of their children. This policy is designed primarily to safeguard students, but also to provide guidance for adults in positions of responsibility. It applies to all members of the Summer School community, including students, teachers, activity leaders, house parents, support staff, visitors, volunteers and temporary staff. It is not limited to the Summer School network; it is designed to cover all aspects of Online Safety that may impact on the Summer School community. It should be read in conjunction with the Safeguarding Policy, the Staff Handbook and the Student & Parent Handbook, which are available on the Summer School Website.

We recognise that, due to the quickly evolving nature of this subject, terminology is likely to change frequently. This policy will, therefore, be subject to a thorough review on a yearly basis to address the fast-changing nature of the subject.

As with all aspects of safeguarding and our strong focus on pastoral care, all members of staff have a responsibility to promote awareness and compliance with the terms of this policy.

Education and Awareness

The Summer School considers itself to have a central role in educating students, parents and staff in issues that may affect them in this area.

Students
During their induction, students are introduced to technical and behavioural aspects of online safety; are made aware of internet protocol whilst at the school and are informed who to speak to if they have any issues or concerns.

Staff
As part of mandatory Safeguarding training, existing Whitgift staff have received formal Online Safety training. New staff receive Online Safety training as part of their induction.

Parents
There may be a gap between some parents' awareness of safety issues, and the technical proficiency of their children. Should parents have any concerns over, or wish to seek guidance on any aspect of Online Safety, they are encouraged to contact the Course Director or the Welfare Manager.

Should parents have concerns that their child has been subjected to attempts at sexual grooming, radicalisation, or other inappropriate online contact, they should contact the Course Director or the Welfare Manager as a matter of high importance. The Welfare Manager is the Safeguarding Lead and will, where appropriate, liaise with outside agencies, such as social services, the police and in particular the CEOP (Child Exploitation and Online Protection) service, (details of which can be found at www.ceop.police.uk)

Should parents wish to discuss any other aspect of online behaviour, such as possible online gaming addiction, or concerns about the amount of time spent online, they should contact the Course Director or the Welfare Manager as a matter of importance.

The School Network, Social Media and related issues

The School is responsible for ensuring the School Network is as safe and secure as possible, and undertakes to filter content, denying access to material that might prove offensive, inappropriate, or harmful. These filters are reviewed regularly, but the School cannot guarantee that such material is always inaccessible. Students are expected to adhere to the Acceptable Use Policy, as published in the Appendix. Filtering is such that it does not 'over block' or restrict access.

The School will monitor the use of communications and online behaviour for all users of the system in order to best ensure that the online environment remains both safe and secure.

Staff
It is the responsibility of all staff to adhere to the Safeguarding policies, and these apply just as much to the use of ICT systems, either those in the School Network, or outside of it. The three principles of *Prevention*, *Protection* and *Support* should determine any action taken by a member of staff.

If members of staff wish to seek guidance on any aspect of Online Safety, they should consult the Course Director or Welfare Manager.

Communication between staff and students
All staff should maintain an appropriate relationship between themselves and students in accordance with the Summer School's Code of Conduct. They must also be aware of the potential for this relationship to become blurred if they use social media that are not visible to the Summer School. As a result, for communication with students they should only use media

that are under the regulation of the School Network. Currently, this is restricted to the School email.

Should members of staff wish to use any other form of communication, they must gain express permission from the Course Director.

Similarly, all staff should be aware of their use of private mobile telephones, for written or oral communication, with students. They should ensure that any communication adheres to the Summer School's published guidelines on mobile telephone usage, in the Mobile Devices Acceptable Usage Policy (see Appendix 2).

Professional Standards
Staff should be aware of the potential audience of any social media services that they use in their professional or private capacity, and maintain standards of professionalism in keeping with their position in the Summer School. They should be especially mindful of those services that allow content to be broadcast without discrimination, and of the potential impact on themselves and the School.

Students
It is a guiding principle of the Online Safety policy that the safeguarding of all members of the community should be led by awareness of the issues, and a sense of responsibility from the students about how to behave in any given situation. Whilst the School has control of its own Network, the wide availability of the internet means that technological restrictions on behaviour can only go so far. The Summer School's focus is very much on creating awareness, education, and a sense of responsibility.

Use of Mobile Phones, ICT Systems and laptops
Students are expected, at all times, to adhere to the Mobile Devices Acceptable Use Policy, as set out in the Summer School Rules Student & Parent Handbook. Similarly, the ICT Acceptable Use Policy applies to usage of both the School's systems, and to any privately owned device capable of accessing the internet.

Just as the Summer School's Safeguarding Policy still applies when a student passes beyond the School gates, so these policies similarly still apply when the student is using internet services other than the School Network. The Summer School reserves the right to be involved when it is aware of any behaviour that breaches these policies, and which affects members of the Summer School community or brings the reputation of the Summer School and Whitgift School into disrepute.

Online Bullying
Bullying by text, e-mail, phone call, or social media often leaves no physical scars but can be highly intrusive and hurtful. The Summer School strictly enforces its policies with regard to the use of mobile phones and the internet and monitors closely all online communications used on the Summer School site. The Summer School reserves the right to review electronic material held or accessed by any students in school including their email accounts and their

mobile phones. Should parents feel that their child is involved in Online Bullying, they should report it as soon as possible to the contact the Course Director or the Welfare Manager

Where any form of Online Bullying involves another student, whether the bullying or that student is in the Summer School or another location or may bring the reputation of the Summer School into disrepute, the Summer School reserves the right to be involved, whether the electronic material was produced within the Summer School or outside. Students must be aware that some forms and levels of Online Bullying are illegal and the Summer School will inform the police when necessary.

Radicalisation
Radicalisation is the process by which individuals or groups come to adopt extreme views on political, religious and social matters, notably with the result of violent extremism. The Summer School has a responsibility to protect children from extremist views, and to equip them with the ability to recognise, question and resist any attempts to radicalise during their formative years.

It is expected that anyone is the summer school community will bring to the school's attention any attempts to promote violent extremism.

Accommodation

Because students are on site full time, and the School is therefore also their temporary summer home, there are additional opportunities available to them through the Founder's House wi-fi system, including both educational and recreational use of the internet. In addition, there is the opportunity to communicate with their families by means of Skype, Facetime or similar services. There are specific protocols for online use in Founder's House (see Appendix 3) but students should note that they are also generally bound to observe the terms of the Online Safety Policy.

Reporting Breaches of Online Safety Policy

If any student suspects that a breach of this policy has been made by a member of the Summer School Community, it is their duty to report it as soon as possible to the Course Director or the Welfare Manager

Glossary of Terms used in this Policy

- Social media – Web-based services that allow individuals to create personal profiles, and communicate with others, either selectively (e.g. Facebook) or universally (e.g. Twitter).

- The School Network – The ICT infrastructure, including the Local Area Network and Wireless Local Area Network that allows access to the internet and Local Network.

Management of personal data

The management of personal data in line with statutory requirements is covered by the Data Protection Policy.

Department for Education guidance:

- Keeping Children Safe in Education (September 2016)
- Online Bullying: Advice for Headteachers and School Staff (November 2014)
- Advice for parents and carers on cyberbullying (November 2014)
- The Prevent Duty: Advice to schools on Radicalisation (July 2015)

Reviewed by the Summer School Course Director: December 2017
Next Review: December 2018

Appendix 1: Acceptable use of the School's ICT systems and facilities

Access to the School's computer networks, the School's systems and the use of computing facilities owned by the School are conditional on observance of the following rules:

Users will

- always behave in a sensible, mature way, respecting others at all times
- report any suspected breach of network security to a member of staff
- only use the School computer network for School-related work
- always be courteous and use appropriate language both to those around them and those they contact through the network
- never seek to harass or abuse fellow students or members of staff through the use of obscene or offensive language or images, via either the School systems or personal devices and will report any cases of inappropriate use
- check the copyright status of items to be downloaded – if unsure check with a member of staff
- use any downloaded material in an appropriate manner in their work, always identifying its source and be aware of any copyright issues
- log out on completion of activity at a workstation

<u>Responsible Internet Use</u>

In the course of the School day, users will not

- enter chat rooms
- play web-based games
- leave stations unattended whilst connected to the internet
- use the School systems for any use that could be deemed inapporpriate

Important notes

- The network is backed up every evening by the School – this means that most files can be restored if deleted or lost in error. This does not apply to files created and deleted on the same day
- The School monitors by electronic means the use of the School's computer systems and web-sites, and to delete inappropriate materials in circumstances where it believes inappropriate use of the School's computer systems is or may be taking place
- **Irresponsible use will result in disciplinary action**

Appendix 2: Mobile Devices – Acceptable Use Policy

Rationale

Whitgift Summer School embraces the use of technology for educational purposes and staff have available to them a variety of mobile devices to enhance Teaching and Learning and administration in a controlled and meaningful way. We also recognise that students' own mobile devices, especially mobile phones, are a central part of their lives and can be, if used responsibly, a valuable tool for communication and information gathering.

The Summer School also has to be aware of the potential misuse of mobile devices and we only allow students to use their own device in particular and tightly controlled circumstances as outlined in this Acceptable Use Policy. Reasons for this include:

- Unregulated use of mobile devices during the day disrupts Teaching and Learning
- Texting and other electronic communication can be used for Online Bullying
- Use of audio or video capabilities can be malicious and used for offensive purposes
- Mobile devices are often valuable items which can go missing
- They also constitute an attractive target for thieves

Procedures

Mobile devices, including mobile phones, tablets and laptops, are brought to Whitgift Summer School entirely at the owner's own risk. The Summer School does not accept responsibility for mobile devices. The Summer School cannot retain mobile devices for safe-keeping during the day.

It is recommended that mobile phones should be made secure in a bedroom locker during the entirety of the Summer School Day. In particular they should not be left unattended in changing rooms or in pockets.

Mobile phone use is prohibited in morning English classes, English in Action classes, mealtimes and afternoon and evening activities. Phones must remain switched off and should not be visible during these times unless students are granted express permission by a member of staff to use their phone for a specific purpose.

We would like students to keep mobile phone use to a minimum during their stay in the boarding house and instead encourage them to communicate face-to-face with the other students. However, it is understood that students will be keen to use them to contact home, and recreationally, and, as such all students are able to access the Boarding House Wifi at set times. However, it is a requirement mobile phones are switched off after lights out to ensure that students are suitably rested.

WHITGIFT

All students using mobile phones at Summer School are reminded of the necessity to use their phones in a mature and responsible manner. Calls and text messages of an abusive nature are illegal and will be deemed a serious breach of Summer School discipline.

The following are strictly forbidden as outlined in the Summer School Rules:

- Use of mobile devices for the storage and/or distribution of offensive (including pornographic) material
- Taking photos or video or audio recordings of fellow members of the Summer School community without express permission for a specific purpose
- Use of mobile devices in any way that may cause embarrassment or discomfort to fellow members of the Summer School community
- Use of 3G or 4G to access inappropriate material

Any mobile phone which is used inappropriately during the Summer School day will be confiscated by staff and will be handed to the Director of Studies, Activity Manager or the Welfare Manager who will retain the phone for a period of time, which may be at least a week. Parents are encouraged to make alternative arrangements for such an eventuality. Serious or repeated offences will result in the privilege of using a mobile phone at the Summer School being withdrawn.

Students are reminded that if they need to make a phone call in an emergency at any time they can do so by speaking to their EAL Teacher, Activity Leader or the Summer School Office.

Appendix 3: Boarding House Internet Protocol

Acceptable Use Policy for Whitgift IT Systems

1. Introduction
In addition to access to Whitgift-owned IT systems, **B**ring **Y**our **O**wn **D**evice is available in the Boarding House. This gives students access to a filtered and monitored internet connection within this building from their own devices (smartphones, laptops, McBooks, tablets, e-readers or any other device capable of accessing the internet.)

The Acceptable Use Policy is designed to set out a framework for responsible use of technology and to ensure the safety and privacy of our students and staff.

2. Definitions used
BYOD: an acronym for Bring Your Own Device. Students are encouraged to bring their own devices for homework, research, entertainment and communication purposes.

Access: wireless connection to the internet via the "Whitgift-BYOD" wireless network or wired/wireless connections via Whitgift-owned equipment. All access may be monitored and/or recorded for network security and student safety purposes.

3. Security and Damages
The student is responsible for the safety and security of any device that they bring to the Boarding House and we recommend that skins or cases are used to physically identify your device from others. We also encourage the use of protective cases.

4. Guidelines
- All network access is filtered and students must not attempt to bypass these systems.
- Computers will not be left unattended whilst connected to the internet.
- Any attempts to bypass security to access systems, hardware or data will be a disciplinary matter.
- The student is fully responsible at all times for their own devices. Whitgift Summer School is not responsible for any loss/damage/theft of a personally owned device.
- The student is responsible for ensuring that the device remain free from viruses and malware, where appropriate installing anti-virus and anti-malware software and security updates.
- No device, personal or otherwise, may be used to record, store or transmit any type of image, sound or video from Whitgift Summer School without the express permission of a member of staff.
- All communications sent using Whitgift's network will befit the image of the Summer School and use appropriate language.
- Users will never seek to harass or abuse fellow students or members of staff through the use of obscene or offensive language or images, either on the School network itself or via the School's systems and will report any cases of inappropriate use

- Be aware of the copyright status of any items downloaded or viewed on the internet – if unsure, check with a member of staff.
- Any downloaded material used in Summer School work is to be identified with a credit to the original author.
- "Relaxed" internet access is available to access games, social media and entertainment websites at the following times:
    - Monday, Tuesday, Thursday and Friday: 15:45-16:15, 17:45-18:45, 21:30-22:30
    - Wednesday: 17:45-18:45, 21:30-22:30
    - Saturday and Sunday all day until 18:30, 21:30-22:30
- If we have reasonable suspicion that the student has violated the terms of this agreement, or other Summer School policy, the student's device may be inspected and/or confiscated. Further misuse may lead to the removal of access to Whitgift's IT systems.