WHITGIFT

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 pupils, but also to provide guidance for adults in positions of responsibility. It applies to all members of the school community, including pupils, teachers, support staff, visitors, volunteers and temporary staff. It is not limited to the school network; it is designed to cover all aspects of Online Safety that may impact on the school community. It should be read in conjunction with the Safeguarding Policy and the Pastoral Handbook, which are available on the 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 School considers itself to have a central role in educating pupils, parents and staff in issues that may affect them in this area.

Pupils

The School provides a programme that raises awareness of technical and behavioural aspects of safety for pupils, including topics such as advice on grooming and radicalisation, exposure to material that is not appropriate to their age, the sharing of personal information, and their online footprint. This is delivered throughout the curriculum generally, and specifically in PSHEE, Critical Reflection and ICT periods, as well as assemblies. The programme is designed to deliver information and explore issues at a level appropriate to the age of the pupil, and certain topics will be revisited at appropriate points in their development.

Staff
Both as part of mandatory Safeguarding training, and the INSET programme, staff receive 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. Therefore, the school provides information and guidance to help bridge this gap through a variety of means, including SchoolPost, letters, newsletters, the School Website, the Virtual Learning Environment and Parents' Evenings. Should parents have any concerns over, or wish to seek guidance on, any aspect of Online Safety, they are encouraged to contact their son's Form Tutor, Head of Year, the Online Safety Co-ordinator, Ms K. Goldberg, ktg@whitgift.co.uk, or the Assistant Head (Pastoral), Mr S. Cook sdc@whitgift.co.uk. The School believes that communication between home and school is vital in the establishment of good Online Safety principles and practice.

Should parents have concerns that their son has been subjected to attempts at sexual grooming, radicalisation, or other inappropriate online contact, they should contact the relevant Head of Year, the Online Safety Co-ordinator or the Assistant Head (Pastoral) as a matter of high importance. The Assistant Head (Pastoral) 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 similarly contact any of the relevant staff 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 given training on how to keep safe online, and what to do should they find inappropriate material. Furthermore, they 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. Filtering reports will be monitored and checked regularly by the Designated Safeguarding Lead (Assistant Head Pastoral) and the Second Master and any issues will be followed up.

All users are provided with a username and password, and will have clearly defined access rights to the school ICT systems. 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.

The "master/administrator" passwords for the school ICT systems, used by the IT Support Team are available to the Second Master and kept in a secure place.

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 Assistant Head (Pastoral) or the Online Safety Co-ordinator.

Communication between staff and pupils
All staff should maintain an appropriate relationship between themselves and pupils, in accordance with the 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 school. As a result, for communication with pupils they should only use media that are under the regulation of the School Network. Currently, this is restricted to:

- school email
- Firefly messaging service

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

Similarly, all staff should be aware of their use of private mobile telephones, for written or oral communication, with pupils. They should ensure that any communication adheres to the 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 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.

Pupils
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 pupils 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 School's focus is very much on creating awareness, education, and a sense of responsibility.

The School believes firmly in the principle of a pupil voice to address concerns and seek guidance for pupils on aspects of Online Safety that directly affect them. It encourages all members of the School Community to feed back on issues in PSHEE lessons, Year Committee Meetings, and Parents' Evenings.

Use of Mobile Phones, ICT Systems and laptops

Pupils are expected, at all times, to adhere to the Mobile Devices Acceptable Use Policy, as set out in the School Rules and regulations. 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.

In particular circumstances, such as when recommended by the Learning Support Department, certain pupils are permitted to use laptops in lessons and generally on the School site. In all cases, such use is bound by the terms of this policy and of the Acceptable Use Policy (see Appendix 1).

Just as the School's Safeguarding Policy still applies when a pupil passes beyond the School gates, so these policies similarly still apply when the pupil is using internet services other than the School Network. The School reserves the right to be involved when it is aware of any behaviour that breaches these policies, and which affects members of the School community or brings the reputation of the 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 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 School site. The School reserves the right to review electronic material held or accessed by any pupils in school including their email accounts and their mobile phones. Should parents feel that their sons are involved in Online Bullying, they should report it as soon as possible to the relevant Head of Year, the Online Safety Co-ordinator or the Assistant Head (Pastoral).

Where any form of Online Bullying involves another pupil, whether the bullying or that pupils is in the School or another school or may bring the reputation of the School into disrepute, the School reserves the right to be involved whether the electronic material was produced within the School or outside. Pupils must be aware that some forms and levels of Online Bullying are illegal and the 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 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.

The School therefore monitors its filtering systems for attempts made online by those wishing to radicalise others, educates on how to recognise these attempts, promotes critical thinking through the PSHEE and Critical Reflection curriculum. It is expected that anyone in the community will bring to the School's attention any attempts to promote violent extremism.

Boarding

Because most Whitgift boarders are on site full time, and the School is therefore also their term-time 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 pupils 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 pupil suspects that a breach of this policy has been made by a member of the School Community, it is his duty to report it as soon as possible to his Form Tutor or Head of Year, or in the case of a breach in the boarding house, to the Housemaster of Founder's House.

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).
- Virtual Learning Environment (VLE) – a software system designed to support teaching and learning in an educational setting – Firefly is currently used.
- 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 (May 2016 for implementation 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 Online Safety Co-ordinator: August 2016

Next Review: August 2017

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

Access to the School's computer networks, the School's systems including Firefly, 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
- only log on using their own username and keep their password secret
- 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
- organise their network space efficiently and delete unwanted files

Responsible Internet Use

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

When using the messaging function in the School's Firefly system

- will compose messages carefully and politely (As messages may be forwarded, e-mail is best regarded as public property)
- gain access to the facility via their username and password, which must not be given to any other person
- will not instigate "mass" messages and chain letters

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, including Firefly 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 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 pupils' 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 School also has to be aware of the potential misuse of mobile devices and we only allow pupils to bring in 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 in School
- They also constitute an attractive target for thieves both when the devices are left at School and on the journey to and from School
- Public Examination Boards regard mobile devices as a threat to exam security

Through our pastoral and curricular programme we aim to educate the boys in responsible use of technology; for further details see the Online Safety Policy.

Procedures

Mobile devices, including mobile phones, tablets and laptops, are brought to Whitgift entirely at the owner's own risk. The School does not accept responsibility for mobile devices and parents should consider adding mobile devices to their house insurance in case of loss. The School cannot retain mobile devices for safe-keeping during the day. Pupils who have express permission to bring such devices (e.g. on the advice of the Learning Support department) must ensure that they are for their own use only and the devices are kept secure at all times. Games consoles and digital cameras are not permitted at any time.

<u>For pupils in the Lower First – Upper Fifth Forms</u>
It is recommended that mobile phones should be made secure in a locker during the entirety of the School Day. In particular they should not be left unattended in changing rooms or in blazer pockets. Mobile phone calls may not be made from School between 8.25 a.m. and 3.45 p.m. without the express permission of a member of staff.

<u>For pupils in the Sixth Form</u>

Members of the Sixth Form are permitted to use mobile phones only within the Sixth Form Centre before and after school and during morning and lunch breaks. At all other times, however, they must have their phones switched off. They must not use their

phones in public areas including corridors and the Dining Hall. Their phones must remain switched off in lessons at all times unless they are granted express permission by a member of staff to use their phone for a specific purpose.

No mobile phone should be visible outside the times and locations where use is permitted.

All pupils using mobile phones at 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 School discipline.

The following are strictly forbidden as outlined in the 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 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 School community
- Use of 3G or 4G to access inappropriate material

Any mobile phone which is used inappropriately during the School day will be confiscated by staff and will be handed to the Head of Year or Assistant Head 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 bringing a mobile phone to School being withdrawn.

Pupils 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 Head of Year or the School Office.

Boarders

The arrangements for use of mobile devices for Boarders when they are in the Boarding House is different and Boarders should refer to the Boarding House Acceptable Use Policy and the Boarders' Handbook for further details.

Appendix 3: Boarding House Internet Protocol (see ADN/RGM)

Boarding Students: 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 now available for Whitgift's boarding students in the Founder's House. This will give all boarding students access to a filtered and monitored internet connection within this building from their own devices.

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. With the opening of the Founder's House, boarding 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 Founder's 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

- In order to access Whitgift's IT systems and services boarding students must review and sign the Acceptable Use Policy.
- All network access is filtered and students must not attempt to bypass these systems. A check on the filtering is regularly made by the Designated Safeguarding Lead (Assistant Head Pastoral) and the Second Master and any issues will be followed up.
- User accounts must not be shared and passwords must remain secret.
- 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 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.
- The use of personal devices is limited to the Founder's House.
- No device, personal or otherwise, may be used to record, store or transmit any type of image, sound or video from Whitgift School without the express permission of a teacher.

- All communications sent using Whitgift's network will befit the image of the 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 Schoolwork is to be identified with a credit to the original author.
- Network storage space is to be used efficiently and files should be deleted when no longer required.
- "Relaxed" internet access is available for Boarders to access games, social media and entertainment websites at the following times:
    - Monday to Friday: 13:00-14:00, 16:00-17:30, 20:00-23:00.
    - Saturday and Sunday all day.
- If we have reasonable suspicion that the student has violated the terms of this agreement, or other 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.