WHITGIFT

ONLINE SAFETY POLICY

Introduction

Whitgift embraces the benefits that technology can bring to staff and student outcomes. 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, such as instances of sexual grooming via chatrooms, and strong evidence of online strategies being employed to radicalise young people. This policy is designed primarily to safeguard students, but also to provide guidance for all adults who interact with students. It applies to all members of the school community, including students, 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 students, parents and staff in issues that may affect them in this area. We cover online safety content within the PSHEE programme (named Ideatum), which is reinforced within a wider, whole school approach. We consider vulnerable students (e.g., SEND or those being bullied/bullying) and use of external visitors to deliver expert training. We also consider the content of external teaching materials to ensure students are taught about online harms and risks in a safe way. We note that the breadth of issues classified within online safety is considerable but can be categorised into three areas of risk which staff and students should be aware of:

- Content: being exposed to illegal, inappropriate, or harmful material; for example, pornography, fake news, racist or radical and extremist views.
- Contact: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, or online bullying.

Students

The School provides a programme that raises awareness of technical and behavioural aspects of safety for students, 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 Ideatum, as well as assemblies. The programme is designed to deliver information and explore issues at a level appropriate to the age of the student, and certain topics will be revisited at appropriate points in their development.

Staff

New staff receive Online Safety training, as part of their induction. It is also mentioned during mandatory safeguarding training for all staff. Where relevant, it is also discussed in the Pastoral Update to all staff, which is compiled each week by the Deputy Head (Pastoral).

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 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 Head of Online Safety, Mr R. Flook rmf@whitgift.co.uk or the Deputy Head (Pastoral), Mr D. Kirby dmk@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 or has received illegal content, they should contact the relevant Head of Year, the Head of Online Safety or the Deputy Head (Pastoral) as a matter of high importance. The Deputy 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.

<u>The School Network, Social Media and related issues</u>

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 Student Acceptable Use Policy, as published in the Appendix 3. Filtering is such that it does not 'over block' or restrict access. Filtering reports are overseen by the Head of Online Safety, and where safeguarding concerns arise, these are highlighted to the Designated Safeguarding Lead (Deputy Head (Pastoral)) and to the Senior Deputy. Any issues will be followed up from an educational and disciplinary perspective.

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 Senior Deputy 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 Deputy Head (Pastoral) or the Head of Online Safety.

Communication between staff and students

All staff should maintain an appropriate relationship between themselves and students, 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 students they should only use media that are under the regulation of the School Network. Currently, this is restricted to:

- school email
- Firefly messaging service
- Microsoft Teams

Should members of staff wish to use any other form of communication, they should seek the advice of the Head of Online Safety and must gain express written permission from the Senior Deputy.

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 School's published guidelines on mobile telephone usage, in the Mobile Devices Acceptable Use Policy (see Appendix 1).

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.

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

The School believes firmly in the principle of a student voice to address concerns and seek guidance for students 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

Students 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 students 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 Student Acceptable Use Policy (see Appendix 3).

Just as the 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 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 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.

If The School reasonably suspects an electronic device has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so. This may extend to online accounts, depending on the nature of the concern, or the likelihood of potential harm.

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 Head of Online Safety or the Deputy Head (Pastoral).

Where any form of Online Bullying involves another student(s), whether the bullying or that student(s) 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. Students 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 Ideatum 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 Boarding House Acceptable Use Policy in Appendix 2) 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 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 – Online 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 suite of common platforms (e.g. Office365), 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 2023)
- Preventing and Tackling Bullying: Advice for Headteachers and School Staff (July 2017)
- Advice for parents and carers on cyberbullying (November 2014)
- The Prevent Duty: Advice to schools on Radicalisation (July 2015)
- Education for a Connected World – This provides age specific advice about the online knowledge and skills that students should develop at different stages of their lives.

Reviewed by Head of Online Safety: September 2023

Next Review: September 2024

Appendix 1: 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 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 School also has to be aware of the potential misuse of mobile devices and we only allow students to bring in their own devices 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 cyber-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 examination security
- There is growing concern about the overuse of mobile devices, potentially leading to unhealthy habits

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

Procedures

Mobile devices, including mobile phones, 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. Students who bring such devices (e.g. on the advice of the Learning Support Department) must ensure that they are for their own use only and that the devices are kept secure at all times. Games consoles are not permitted at any time.

For students in the Lower First (Year 6) to Fifth Forms (Year 11)

Mobile phones should be kept securely during the entirety of the school day. In particular, they should not be left unattended in changing rooms or in blazer pockets. No mobile phone should be visible outside the times and locations where use is permitted. Students should always ask a member of staff if they can use their phone (for example, to check a timetable). If students do not have the permission of a member of staff, they will be asked to put their phone away and this will be logged on iSams. If this happens multiple times, there will be a greater sanction.

Upon arrival at school: phones should be put away by the top of the school drive (Terrace) and at the back of the school by the Fives Courts.

Upon departure: phones may be used when you are outside the building and departing the school site (but not in classrooms if you are waiting for a school bus).

For students in the Sixth Form (Years 12 and 13)
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. They must not use their phones in public areas, including corridors and the Dining Hall. Their phones must remain switched to silent in lessons at all times, unless they are granted express permission by a member of staff to use their phone for a specific purpose e.g. taking a picture of the board or for quick research on the Internet.

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

All students using mobile phones at School are reminded of the necessity to use their phones in a mature and responsible manner. Calls and 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 photographs or making video or audio recordings of fellow members of the School community (this includes all staff) 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,4G or 5G to access inappropriate material

Any mobile phone which is used inappropriately during the School day will be confiscated by staff and handed to the Head of Year or Assistant Head (Pastoral and Boarding). They will retain the phone for a period of time, which may be a week, depending on previous breaches of the School rules regarding the use of mobile phones. Serious or repeated offences will result in the privilege of bringing a mobile phone to 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 Head of Year.

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 (see Appendix 2) and the Boarders' Handbook for further details.

Appendix 2: Boarding House Acceptable Use Policy

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This document is specifically applicable to using the school network and your own devices when in the boarding house. This document is to be adhered to, alongside the general student AUP.

- I will be a responsible user and stay safe when using the internet and other digital technology in the boarding house.
- I will ensure that my online activity or use of mobile technology, on school grounds or outside, will not cause my school, the staff, students, or others distress or bring the school into disrepute.
- I will ensure that I will hand in personal devices in relation to the house rules for lights out.
- I understand that all internet and device use in school is subject to filtering and monitoring; I understand that all school-owned devices used in the boarding house may also be subject to filtering and monitoring and should be used as if I am in school.
- I will keep my logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it.
- I will not bring files into school or download files that can harm the school network or be used to bypass school security.
- I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
- I will use the internet, games and applications responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
- I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
- I understand that some material is intended for adult audiences and I will not download or access this material using my own devices, a school device or through the school network.
- I understand that cyberbullying is unacceptable, and will not use technology to bully, impersonate, harass, threaten, make fun of, or upset anyone, at school or outside.
- I will not browse, download, upload, post, retweet or forward material that could be considered offensive, harmful or illegal. If I come across any such material, I will report it immediately to a member of staff.
- I will only use school e-mail or other communication applications for contacting people as part of learning activities.
- The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
- I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
- When using the internet, I will not download copyrighted material (text, music, video etc.)

- I will not share my or others' personal information that can be used to identify me, my family, or my friends on any online space, unless a trusted adult has given permission.
- If plan on live streaming, I will tell a trusted adult about it.
- I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.
- I will only use my personal devices (mobile phones, USB devices etc) in school if I have been given permission to do so.
- I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting inappropriate photos.
- When using digital devices for recreational activities (e.g. games consoles, my personal laptop), I will use the device and platform in a mature and considered way.
- I understand that many applications have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, so it is not too easy to find out where I live or go to school.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, extremist/hateful content, I will not respond to it but I will save it and talk to a trusted adult.
- I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
- I know who my trusted adults are at school, home and elsewhere, but if I feel I cannot talk to them, I know I can call Childline or click CEOP.
- I understand that I am responsible for the security and safety of my own devices and that personal devices should have protected cases where possible and all personal devices should be labelled with my name.
- The use of VPNs is prohibited on any device which connects to the school network/WiFi.

I have read and understand these rules and agree to them.

Name: ___________________________________

Signed: __________________________________

Date: ___________________

Appendix 3: Student Acceptable Use Policy

These rules will help to keep everyone safe and ensure fairness to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

1. I will be a responsible user and stay safe when using the internet and other digital technology at school.
2. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
3. I will only use the school's internet and any device I may be using in school for appropriate school activities and learning, unless I have express permission to carry out recreational activities, e.g. in a lunchtime club or after school.
4. I understand that all internet and device use in school is subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used as if I am in school.
5. I will keep my logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it.
6. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
7. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
8. I will use the internet, games and applications responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
9. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
10. I understand that cyberbullying is unacceptable, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside.
11. I will not browse, download, upload, post, retweet or forward material that could be considered offensive, harmful or illegal. If I come across any such material I will report it immediately to my teacher or Head of Year.
12. I will only use school e-mail or other communication applications for contacting people as part of learning activities.
13. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
14. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
15. When using the internet, I will not download copyrighted material (text, music, video etc.)
16. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
17. If I plan on live streaming, I will tell a trusted adult about it.
18. I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.

19. I will only use my personal devices (mobile phones, USB devices, etc.) in school if I have been given permission to do so.
20. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting inappropriate photos.
21. I understand that many applications have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, so it is not too easy to find out where I live or go to school.
22. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
23. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, extremist/hateful content, I will not respond to it but I will save it and talk to a trusted adult.
24. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
25. I know who my trusted adults are at school, home and elsewhere, but if I feel I can't talk to them, I know I can call Childline or click CEOP.

I have read and understand these rules and agree to them.

Name: ___________________________________

Signed: __________________________________

Date: ___________________