

WHITGIFT SUMMER SCHOOL

ONLINE SAFETY POLICY

Introduction

Whitgift Summer School recognises the vast opportunities that the internet and digital technologies offer to both staff and students. However, we also acknowledge the associated risks, including but not limited to instances of sexual grooming via chatrooms, bullying, stalking, radicalisation, sextortion, AI deepfakes and identity theft. We are committed to raising awareness of the potential risks ensuring that our students are equipped with the knowledge, skills, and support necessary to navigate the online world safely and responsibly.

Whitgift School understands its responsibilities include:

- Education and Awareness: Providing students with age-appropriate education on online safety, including critical thinking skills and responsible digital behaviour, to enable them to remain safe and within the law when using the internet and related technologies in and beyond the classroom.
- Student Voice and Engagement: Creating opportunities for students to discuss online safety concerns, share their experiences, and contribute ideas to improve our digital safeguarding practices.
- Safe Online Environment: Maintaining a secure and monitored online environment within the School's digital infrastructure to protect students from potential harm.
- Intervention and Support: Implementing effective mechanisms to identify, respond to, and escalate online safety concerns promptly and appropriately.

This policy is designed to safeguard the welfare of all students, provide a framework for the safe and responsible use of IT systems, and to clearly define individual responsibilities. It aims to:

- Provide clear guidance on how to minimise risks associated with online activity.
- Outline what is deemed in our context as acceptable behaviour and digital conduct.
- Establish clear structures by which online misdemeanours will be treated.
- Define the procedures for responding to online safety, particularly where there are doubts or concerns.

Online safety is a continuous and interconnected theme across many of Whitgift School's policies. This document should be read in conjunction with other school policies, including but not limited to:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour, Discipline and Exclusions Policy
- Social Media and Communications Policy
- AI Policy
- Summer School Staff Handbook
- Summer School Student and Parent Handbook

All available on the Whitgift School Website.

Whitgift Summer School recognises that, due to the quickly evolving nature of the online environment, terminology and technology is likely to change frequently and present new emerging risks. This policy is therefore subject to a thorough annual review.

In addition to scheduled reviews, the policy will be updated as necessary in response to any new technological developments, emerging threats to online safety, or specific incidents or concerns arising within the School or the wider educational context.

Roles and Responsibilities

Online safety is a shared responsibility. To ensure the safeguarding of all members of the school community, it is important the whole community works together to:

- Model and develop safe and responsible online behaviours
- Promote awareness, understanding and learning from each other of online risk.
- Reporting inappropriate online behaviours, concerns, or misuse as soon as they become apparent.
- Support one another in developing digital resilience.

Students

Students are expected to take an active role in maintaining a safe and respectful online environment. During their induction, students are introduced to technical and behavioural aspects of online safety, made aware of internet protocol whilst at the school and informed of whom to speak to if they have any issues or concerns. Key responsibilities include, but are not limited to:

- Using the internet and technology in accordance with the Schools' and Summer Schools' policies
- Knowing what action to take if they or someone they know feels worried or vulnerable when using online technology
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of staff.

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.

It is the responsibility of all staff to adhere to the Summer School Safeguarding and Child Protection 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.

In addition, they

- Must be aware that technology can play a significant part in many safeguarding and wellbeing issues and that students are at risk of abuse online as well as face-to-face. Staff must also be aware that, sometimes, such abuse will take place concurrently online and during a student's daily life.
- Are expected to be alert to the possibility of students abusing their peers online and to understand that this can occur both inside and outside of school.
- Are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in and outside classrooms and to model positive attitudes and approaches to online safety.

As with all aspects of safeguarding and our strong focus on pastoral care, all staff

members are responsible for promoting awareness and compliance with this policy. If members of staff wish to seek guidance on any aspect of Online Safety, they should consult the Course Director or Welfare Manager (DSL).

Parents

The role of parents in ensuring that their child understands how to stay safe online as well as promoting safe and responsible practice in their own use of technology is crucial.

Whitgift Summer School will contact parents if it has any concerns about students' online behaviour and likewise hopes that parents will feel able to share any concerns with the School.

Should parents have concerns that their child has been subjected to attempts of sexual grooming, radicalisation, sextortion/extortion, or other inappropriate online contact, or they have received illegal content, 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 Multi Agency Safeguarding Hub (MASH), 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.

Education and Awareness

Whitgift Summer School considers itself to have a central role in educating students, parents and staff in online safety issues that may affect them.

The breadth of issues classified within online safety can be categorised into four areas of risk, which staff, parents/carers and students should be aware of:

- **Content:** being exposed to illegal, inappropriate, or harmful material (e.g. pornography, fake news, racist or extremist views, suicide)
- **Contact:** being subjected to harmful online interaction with other users (e.g. Online grooming incl. sexual exploitation, radicalisation, personal data exploitation)
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending, and receiving explicit images, or online bullying)
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The School Network, Social Media and related issues

The School understands its responsibility for ensuring that the School's IT infrastructure is as safe and secure as is reasonably possible and aims to provide a safe environment to learn and work, including when online.

The School provides internet access and an email system as well as other technology to students and staff. It 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 Policies, as published in the Appendices. 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.

Any issues will be followed up the Welfare Manager (as Designated Safeguarding Lead) and Course Director.

Communication Between Staff and Students

Any digital communication between staff and students or parents must be professional in tone and content. All staff should maintain an appropriate relationship between themselves and students in accordance with the Summer School course specific Code of Conduct and Social Media and Communications Policy. They must also be aware of the potential for this relationship to become blurred if they use social media that is not visible to Whitgift Summer School.

For communication with students, staff should only use systems that are under the regulation of the School network. This is for the mutual protection and privacy of all staff, students and parents, supporting safeguarding best-practice. Currently, this is restricted to:

- the School's email system (Outlook)
- Microsoft Teams

The School recognises though that there are situations (for example, in emergencies) where there may be no alternative.

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

Any accidental use of a personal email address or telephone number to communicate with students or parents should be reported in line with the School's Low-Level Concerns Policy.

Professional Standards

Staff should be aware of the potential audience of any social media services that they use in their professional or private capacity, maintaining the same expected standards of professionalism, as benefitting the position of trust of anyone working on the course. 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.

They must adhere to the standards outlined in the School's Social Media and Communications Policy, Staff and Visitor Acceptable Use Policy as well as the Staff Code of Conduct.

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.

Use of Mobile Phones, ICT Systems and Laptops

Students are expected to adhere to the Mobile Devices Acceptable Use Policy (see Appendix 1) at all times, as set out in the course specific rules, as well as the Student & Parent Handbook. Similarly, the Summer School Acceptable Use Policy (see Appendix 3) and Boarding House Internet Protocol (Appendix 2) applies to usage of both the School's systems, and to any privately owned device capable of accessing the internet.

Just as Whitgift Summer School 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. Whitgift 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 Whitgift Summer School and Whitgift School into disrepute.

Cyberbullying

Bullying by text, electronic messaging, e-mail, phone call, or social media can be highly intrusive and hurtful. Whitgift Summer School strictly enforces its policies regarding the use of mobile phones and the internet and closely monitors all online communications on its network.

If Whitgift Summer 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 child is involved in online bullying, they should report it as soon as possible by contacting the Course Director or the Welfare Manager.

Where any form of cyberbullying involves another student, whether the bullying or that student is in the School or another school, or may bring the School into disrepute, the School reserves the right to be involved. This applies whether the electronic material was produced within the School or outside.

Cyberbullying incidents, including incidents that take place outside school or from home, will be dealt with in accordance with the School's Anti-Bullying Policy and Behaviour, Discipline and Exclusions Policy. Students must be aware that some forms of cyberbullying 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. Whitgift Summer School has a responsibility to protect students from extremist views, and to equip them with the ability to recognise, question and resist any attempts to radicalise them, especially during their formative years.

The internet has made it much easier for radicalisers to find and identify people who might be easily influenced and drawn into extremist behaviour. Anyone can be susceptible to being radicalised regardless of their age, but young people can sometimes be at greater risk.

One function of the School's monitoring is to identify those wishing to radicalise others.

Anyone in the Whitgift Summer School community should bring to the Summer School's attention any attempt to promote violent extremism, as a safeguarding concern, contacting the Welfare Manager (Designated Safeguarding Lead) or the Deputy DSL responsible for Prevent.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at

scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer). Sextortion (Threats to share sexual images or videos of a person unless they meet certain demands such as money, more images, or further communication) is also considered a cyber crime.

The School is aware that students with particular skills and interests in computing and technology can be at risk of straying into cyber-dependent crime.

If staff have any concerns about a child in this area, they should refer the matter to the Director of Safeguarding/DSL immediately who might consider a referral into the Cyber Choices programme, a nationwide police programme supported by the Home Office and led by the National Crime Agency.

Nudes and Semi-Nudes Incidents (Sexting)

The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Staff **must never** view, copy, print, share, store or save the imagery, or ask a child to share or download – this is illegal. If staff viewed the imagery by accident (e.g. if someone has shown it to you before you could stop them), report this to the DSL (or equivalent) and seek support.

Staff must immediately report any incident to the Course Director or Welfare Manager as the Safeguarding DSL who will then follow the UKCIS guidance Sharing Nudes and Semi-Nudes: [How to Respond to an Incident](#). Incidents may also include the sharing of digitally manipulated or AI-generated images.

The sharing of nudes or semi-nudes may constitute a criminal offence and will be considered in accordance with the School's Safeguarding and Child Protection Policy as well as the advice published by the UK Council for Child Internet Safety (UKCIS): [Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People](#). It is important that everyone understands that whilst the sharing of nudes and semi-nudes is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Use of AI and Deepfake Technology

The use of Artificial Intelligence (AI), including generative tools and deep fake technology, presents both opportunities and risks in the context of online safety and safeguarding. In accordance with Keeping Children Safe in Education (KCSIE) 2025, this school recognises the emerging risks associated with AI-generated content, including:

- The potential for misinformation, disinformation, and conspiracy content, which may influence pupils' worldviews and online behaviour.
- The creation and spread of deep fake images, videos, or audio that may be used to bully, harass, deceive, or manipulate others.
- The misuse of AI tools to generate inappropriate or harmful material, including sexually explicit, violent, or extremist content.

If staff have any concerns about a child in this area, they should refer the matter to the Course Director or Welfare Manager as the Safeguarding DSL immediately. Any incidents involving the use of AI will be dealt with by the DSL as well as appropriate staff such as the Director of Studies.

Safe Use of Digital Images

Staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming 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. Staff should inform and educate students about the risks associated with the taking, using, sharing, publication and distribution of images and encourage students to think about their online reputation and digital footprint.

Staff should only use images of students where permission has been obtained, and only for the given purpose.

Photographs chosen to be published on the School's social media platforms and school website must be selected carefully and must never identify a student by full name without specific permission. Please refer to the school's Taking, Storing, Using Images Policy for further information.

Staff, students and parents are reminded of the importance of not sharing without explicit permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

Filtering and Monitoring

Filtering and monitoring are important parts of the School's safeguarding arrangements and it is therefore vital for staff to be aware of the systems in place and to play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking.

Staff, students and visitors should be aware that the School's filtering and monitoring systems apply to all users, all school owned devices and any devices connected to the School's internet. Deliberate access, or an attempt to access prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour, Discipline and Exclusions Policy.

The School is responsible for ensuring that the School network is as safe and secure as possible, and undertakes to filter content without unreasonably impacting teaching and learning and restricting students from learning how to assess and manage risk themselves.

Accommodation

Because students are on site full-time, and the School acts as their temporary home. This means there are additional opportunities available to them through the Founder's House (the boarding house residence) Wi-Fi system. These include both educational and recreational use of the internet, the opportunity to communicate with their families by means of Teams, Zoom, Facetime, WhatsApp or similar services. As a result there are specific protocols for online use in Founder's House (see the Boarding House Internet Protocol in Appendix 2), but students should note that they are also generally bound to observe the terms of this policy.

Reporting Incidents of Misuse of Online Safety Policy

Staff, students and parents/carers are encouraged to report concerns, incidents of misuse or suspected misuse swiftly to allow the School to deal with them quickly and sensitively following the School's safeguarding and disciplinary policies and procedures. It is their duty to report it as soon as possible to the Course Director or the Welfare Manager.

Whitgift Summer School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously.

If a member of staff discovers that a student is at risk as a consequence of online activity, they should report it to the Welfare Manager as soon as reasonably possible who may seek assistance from the [CEOP](#) Safety Centre or other professional advisors as appropriate.

- Anti-Bullying Policy
- Behaviour, Discipline and Exclusions Policy
- Student Acceptable Use Policy
- Staff Code of Conduct
- Staff and Visitor Acceptable Use Policy

Record Keeping

All serious incidents involving the use of technology will be centrally logged and kept as part of the student or staff record.

The information created in connection with this policy may contain personal data. The School's use of personal data will be in accordance with data protection law and in line with the School's data protection policies and procedures. The School has published privacy notices which explain how the School will use personal data.

Management of Personal Data

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

Due regard has been given to the following guidance:

- DfE Cyber Bullying: Advice for Headteachers and School Staff
- DfE Filtering and Monitoring Standards
- UKCIS Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People (March 2024)
- DfE Keeping Children Safe in Education (September 2025)
- DfE Mobile Phones in Schools (February 2024)
- DfE Teaching Online Safety in Schools (January 2023)
- DfE Relationships Education, Relationships and Sex Education (RSE) and Health Education (June 2019, as amended September 2021)
- Prevent Duty Guidance: England and Wales (2023)
- DfE Advice for Parents and Carers on Cyberbullying (November 2014)
- UKCIS Education for a Connected World Framework (2020)
- UKCIS Online Safety in Schools and Colleges: Questions from the Governing Board (2022)
- UKCIS Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People
- UKCIS Using External Expertise to Enhance Online Safety Education (2022)
- UKSIC Appropriate Filtering for Education Settings (2024)
- UKSIC Appropriate Monitoring for Schools (2024)

Reviewed by the Director of International Education: November 2025

Next Review: November 2026

Appendix 1: 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 as well as 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 has to be aware of the potential misuse of mobile devices and we only allow students to use their own device in particular and in 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
- Instant messaging 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
- The use of mobile phones overnight leads to unhealthy levels of tiredness
- There is often a link between high mobile phone use and homesickness
- We want to encourage face-to-face communication throughout our short courses
- Limiting smartphone usage leads to improved wellbeing among students

Procedures

Mobile devices, including mobile phones, tablets and laptops, are brought to Whitgift School entirely at the owner's own risk. Whitgift Summer School does not accept responsibility for mobile devices.

Mobile phones must be kept securely locked away in the boarding house for the entirety of the school day. They should not be left unattended in changing rooms, classrooms, bedrooms or, for example, trouser pockets. Mobile Phone are allowed to be used during free time and taken on excursions.

Use of smartphones and other such like devices is prohibited in all classes, mealtimes and afternoon and evening activities.

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 recreationally and to contact home. As such all students have access the Boarding House Wi-Fi at set times. However, at the Summer School it is a requirement that mobile phones are locked away by the Welfare team before bedtimes. Students should be aware that the Welfare team will not be able to charge phones overnight.

All students using mobile phones at Whitgift 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 discipline.

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

- Use of smartphones and 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 summer school community
- Use of 3G, 4G or 5G to access inappropriate material

Any mobile phone which is used inappropriately or out of the permitted hours 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 smartphone at the school being withdrawn completely.

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 a member of the Welfare Team, who are available at all times to help you over the summer.

Appendix 2: Boarding House Internet Protocol

Acceptable Use Policy for Whitgift IT Systems

1. Introduction

In addition to access to Whitgift-owned IT systems, **Bring Your Own Device** 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, MacBooks, 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 Whitgift 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 school work is to be identified with a credit to the original author.

- If we have reasonable suspicion that the student has violated the terms of this agreement, or other Whitgift Summer School policies, the student's device may be inspected and/or confiscated. Further misuse may lead to the removal of access to Whitgift's IT systems.

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

Name: _____

Signed: _____

Date: _____

Appendix 3: Summer School Student Acceptable Use Policy

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. This document is also applicable to using the school network and your own devices when in the boarding house.

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 Whitgift Summer 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, for example at breaktimes and during free time.
4. I will ensure that I will hand in personal devices in relation to the house rules for lights out.
5. I understand that all internet and devices used in school are subject to filtering and monitoring.
6. 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.
7. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
8. 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.
9. 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.
10. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
11. 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.
12. I understand that cyberbullying is unacceptable and will not use technology to bully at school.
13. 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, the house parents, activity staff or Welfare Manager.
14. 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 Whitgift Summer School.
15. 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.
16. When using the internet, I will not download copyrighted material (text, music, video etc.)
17. 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.
18. If I plan on live streaming, I will tell a trusted adult about it.
19. 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.
20. I will only use my personal devices (mobile phones, USB devices, etc.) in school if I have been given permission to do so.
21. 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.

22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. I understand that the use of VPNs is prohibited on any device which connects to the school network/Wi-Fi.

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

Name: _____

Signed: _____

Date: _____