

# SEVENOAKS SCHOOL SUMMER PROGRAMME

## Online Safety

### Introduction

Sevenoaks School Summer Programme 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 social media, 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 Programme community, including students, teachers, activity leaders, house staff, support staff and visitors. It is not limited to the Summer Programme network; it is designed to cover all aspects of Online Safety that may impact on the Summer Programme community. It should be read in conjunction with the Safeguarding Policy and the Staff Handbook.

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

#### 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 Sevenoaks staff have received formal Online Safety training. New staff receive 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.

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 Director as a matter of high importance. The Director 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](http://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 Director 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. 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 Director.

## **Communication between staff and students**

All staff should maintain an appropriate relationship between themselves and students in accordance with the Summer Programme'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 Programme. As a result, for communication with students they should only use media that are under the regulation of the School Network.

Similarly, all staff should be aware of their use of private mobile telephones, for written or oral communication, with students.

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

### **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 Programme 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 Programme site. The Summer Programme 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 by contacting the Director.

Where any form of Online Bullying involves another student, whether the bullying or that student is in the Summer Programme or another location or may bring the reputation of the Summer Programme into disrepute, the Summer Programme reserves the right to be involved, whether the electronic material was produced within the Summer Programme or outside. Students must be aware that some forms and levels of Online Bullying are illegal and the Summer Programme 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 Programme 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 in the Summer Programme community will bring to the school's attention any attempts to promote violent extremism.

## **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 Programme Community, it is their duty to report it as soon as possible to the Director.

## **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 Instagram) 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.

## **Mobile Devices – Acceptable Use Policy**

Sevenoaks School Summer Programme 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 Summer Programme 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 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
- 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
- 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 the Summer Programme

## **Procedure**

Mobile devices, including mobile phones, tablets and laptops, are brought to Sevenoaks

School Summer Programme entirely at the owner's own risk. The Summer Programme does not accept responsibility for mobile devices. The Summer Programme cannot retain mobile devices for safekeeping during the day.

It is recommended that mobile phones should be kept securely in a bedroom locker when not in use and ideally for the entirety of the Summer Programme day. In particular they should not be left unattended in changing rooms or in pockets.

Mobile phone use is prohibited in classes 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. Teachers and Activity Leaders may collect mobile phones at the beginning of each lesson and activity to help avoid temptation.

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 are able to access the Boarding House Wi-Fi at set times. However, it is an option of the House team for mobile phones to be collected before bedtimes. Phones can be signed back out from the House team each morning before breakfast. Students should be aware that the House team will not be able to charge phones.

All students using mobile phones at the Summer Programme 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 Programme discipline.

The following are strictly forbidden as outlined in the Summer Programme 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 Programme 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 Programme community
- Use of 3G, 4G or 5G to access inappropriate material

Any mobile phone which is used inappropriately during the Summer Programme day will be confiscated by staff and will be handed to the Course Director, Head of Co-Curricular or Head of House who will retain the phone for a period of time. 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 Programme 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 the Director.

## **Boarding House Internet Protocol**

### **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.

### **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. Sevenoaks School Summer Programme 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 Sevenoaks School Summer Programme without the express permission of a member of staff.
- All communications sent using Sevenoaks' network will benefit the image of the Summer Programme 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 Programme 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 Summer Programme policy, the student's device may be inspected and/or confiscated. Further misuse may lead to the removal of access to Sevenoaks' IT systems.