GREENE'S
COLLEGE
OXFORD

E-Safety Policy

This policy was adopted in August 2022.

This policy is due to be reviewed in August 2023.

The person responsible for the implementation of this policy is the College Principal.

It is the responsibility of the College's Governing Body to ensure that this policy is reviewed and updated annually.

Purpose

The purpose of this policy is to:

- ensure the safety and wellbeing of students when using the internet, social media or mobile devices
- provide staff with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all members of the College community (including staff, students and visitors) who have access to and are users of ICT systems in College.

Student responsibility

The most effective form of protection fundamentally lies in the good judgment of students, and is guided by a well-informed understanding of what is available to them and of the risks to which they are potentially exposed. For this reason, we work on the assumption that students must take responsibility for their actions when using the internet. Any misuse of the internet will be dealt with under the College's Code of behaviour or, where relevant, the College's Safeguarding policy.

Bullying

Students must not use their own or the College's devices and technology to bully others. Bullying incidents involving the use of technology will be dealt with under the College's Anti-bullying policy. If a student believes they, or another student has been bullied in this way, they should talk to a member of staff about it as soon as possible.

Abuse

If there is any reason to believe that a student is at risk of abuse from his or her dealings with any form of online activity, including the risk of radicalisation and being drawn to extremist organisations of ideology, the issue will be dealt with under the College's Safeguarding policy. If any student is concerned about something that they have seen on the internet or in a social media context, they must report it to a member of staff about it as soon as possible.

Sanctions

Any non-compliance with College regulations will be dealt with according to the procedures in the College's Behaviour policy. Bullying in any form, including cyberbullying, will be taken very seriously and dealt with appropriately in accordance with the College's Anti-bullying and Behaviour policy. In such cases, the Principal will apply any sanction that is deemed appropriate, including, in the most serious cases, asking a student to leave the College. Where there is reasonable cause to suspect that a student is suffering, or is likely to suffer, significant harm as a result of bullying in any form, including cyberbullying, then the matter will be treated as a safeguarding issue and referred to children's social care or the police.

Acceptable use of the internet

Password security

All students will use their Greene's Online username and password. It is important that students understand the need for complete password security. All students should:

- Use a strong password, which will need to be changed at regular intervals;
- Not write their passwords down;
- Never share passwords with anyone else.

Monitoring and usage

When using the internet, all users are expected to abide by all laws and government regulations concerning copyright, libel, fraud, data protection, discrimination and obscenity. Any attempt to access material which promotes extremism or radicalisation will be taken very seriously and dealt with immediately as set out in the section on 'Preventing radicalisation' in the College's Safeguarding policy. All staff are expected to communicate with students in a professional manner consistent with the guidelines set out in the Code of Conduct for staff at Greene's . Access to the internet is provided to students on the understanding that they will use it in a respectful manner.

Online activities which are not permitted in College

These include:

- Sending, sharing any content that is racist, discriminatory, pornographic, conducive to extremism, violence or radicalisation, or in any way offensive to any other person or group of people, including but not limited to protected characteristics under the Equality Act 2010;
- Sending, copying or displaying offensive messages or pictures, including sexting and so-called nude & semi-nude selfies;
- Using obscene, racist or otherwise discriminatory language;
- Harassing, insulting or attacking others;
- Accessing, or attempt to access, material that promotes extremism and or terrorist activity or organisations, pornography or any other form of harmful, inappropriate or illegal content;
- Copying, saving or redistributing copyright-protected material without approval;
- Publishing, sharing or distributing any personal information about any other user such as home address, e-mail address, telephone number, photographs etc.

Managing e-mail

Students should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. At Greene's this will generally mean they understand that they should tell a member of staff about anything they feel is inappropriate.

Staff should use College e-mail accounts to communicate with students, where possible, and such communications must always be professional in tone, content and motivation.

Managing social media and social networking sites

Students should consider the potential risks with uploading personal information, and the difficulty of removing an inappropriate image or information once online.

- Before students share anything online, they should ask themselves "Is the post caring? Is it true? And is it something I would be happy to be displayed on a large screen in front of the whole school?"
- All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Examples include: blogs, social networking, forums, bulletin boards, chatrooms, instant messaging etc.

- Students are encouraged to set & passwords regularly;
- Posts that, in the reasonable opinion of the College, could be considered offensive to other students will be regarded as a serious breach of discipline and will be dealt with in the context of the College's behaviour policy.

Managing mobile devices

- Students may not bring mobile phones or smart watches into examinations;
- Any student misuse of the internet through internet-enabled devices, such as downloading inappropriate or offensive materials or posting inappropriate comments, in particular racist, pornographic, discriminatory or obscene material, on social networking sites, will be dealt with in accordance with the College's behaviour policy.

Managing photography and video capture on College premises

- Use of photographic material to intimidate, harm or bully other students or staff members will not be tolerated;
- Indecent images taken and sent by mobile devices and other forms of technology (sometimes known as 'Sexting', "nudes" or "semi-nudes") is not permissible, and in some circumstances may be seen as an offence under the Protection of Children Act 1978 and the Criminal Justice Act 1988. If a student thinks that they have been the victim of 'sexting', they should speak to a member of staff about it as soon as possible. This includes upskirting which is a criminal offence;
- If the College has reasonable grounds to believe that a phone, camera, laptop or other device contains images, text messages or other material that may constitute evidence of criminal activity, the College reserves the right to submit such devices to the police for examination.
- Such misuse of equipment may involve removal of the privilege of bringing such devices into College premises on a temporary or permanent basis.

Managing other electronic equipment – eg, laptops, PDAs and tablet computers

- Students can bring other electronic devices such as laptops, PDAs, tablet computers and mp3 players onto College premises, but they remain the responsibility of their owners at all times. They must keep them with them at all times, and they must make sure that they are password protected.

- The College cannot be held responsible for any theft loss of, or damage to, such phones whilst at Greene's.
- No electronic device should be used to bully, harass or intimidate another person whether through text or images. Any such abuse will be dealt with in accordance with the College's behaviour policy.
- No electronic device should contain inappropriate material such as violent or explicit videos or photographs, pornography or any material that could be considered offensive and / or inappropriate in a school context.
- Anti-virus software – student are encouraged to have appropriate anti-virus software that is regularly updated on their laptops;
- Privacy – the College reserves the right to examine the hard drive on a student's personal laptop if there is reasonable suspicion that a computer is being used for inappropriate or harmful purposes on College premises;
- College owned laptops / netbooks – these must only be used for educational purposes. The uploading of inappropriate material such as images, software and graphics is forbidden.

Responses to cyberbullying

It is crucial that students, staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and avoid misuse. Promoting a culture of confident users will support technological development and safety.

- The DfE and Childnet have produced resources that can be used to give practical advice and guidance on cyberbullying. See: https://www.childnet.com/resources/cyberbullyingguidance-for-schools
- Cyberbullying (along with all forms of bullying) will not be tolerated, whether the bullying originates inside or outside of College
- Activities outside of College premises and outside of College hours that in our regard constitute cyberbullying will also be covered by this policy. Instances of cyberbullying will be dealt with according to the College's anti-bullying policy or, where relevant, the College's Safeguarding policy. All incidents of cyberbullying reported to the College will be recorded.

- The College will take reasonable steps to identify the person(s) responsible for any instances of cyberbullying such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary.
- Sanctions may include: Informing parents/guardians, the withdrawal of privileges, eg, to bring a phone into College, the person(s) responsible being asked to remove any material deemed to be inappropriate, temporary or permanent exclusion in the most serious cases, and the Police being contacted if a criminal act is suspected.

Education around e-safety

It is important that the information in this policy is shared with, and understood by all students, staff and also shared with parents and guardians. This is done through:

- Student induction
- Appointment of an E-Safety Officer
- Pastoral conversations (including meetings with Personal Tutors)
- Prompt follow-up in the case of any incidents
- Initiatives and discussions, eg, Safer internet Awareness Day, Anti-bullying week
- Education around safeguarding and wellbeing
- Staff induction
- Ongoing staff training
- Opportunities for staff to seek advice from DSLs and the IT team
- Consistent visual E Safety Guidance Posters are in place in areas where students can have access to digital technologies