GREENE'S TUTORIAL COLLEGE

Oxford

Online Safety (E-Safety) Policy

In line with

360 degree safe

This e-safety policy was adopted on:	*1st August 2019*
The implementation of this e-safety policy will be monitored by the:	*Academic Director reporting to the Governing Body as required*
Monitoring will take place at regular intervals:	*At least once a year*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*August 2021*
In the first instance, should e-safety incidents take place, the following person should be informed:	*Imogen Harris, Academic Registrar*

Scope of the Policy

This policy applies to all members of the college community (including staff and tutors, students, parents and guardians and visitors, etc.) who have access to and are users of the Greene's Online platform and the internet as related to Greene's whether or not on Greene's premises as empowered by the Education and Inspections Act of 2006 and concerning unacceptable behaviour.

This policy includes incidents of cyber-bullying, or other e-safety incidents which may take place off Greene's premises but are linked to membership – in a broad sense – of Greene's. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Greene's will deal with incidents that fall within the scope of this policy and any associated behaviour and anti-bullying policies and may inform parents of incidents of unacceptable e-safety behaviour.

Roles and Responsibilities

The Academic Director is responsible for the E-Safety Policy and for its review and monitoring its effectiveness. The College Principal will be informed about any e- safety incidents and monitoring reports from the Academic Registrar. The Academic Registrar has taken on the role of E-Safety Lead.

The College Principal is also responsible for addressing a serious e-safety allegation being made against a member of staff.

The College Principal:

- takes day to day responsibility for e-safety issues
- liaises with the Director of Studies and Academic Registrar with regard to student involvement in e-safety
- provides training and advice for staff
- liaises with the OSCB

The Academic Registrar also ensures

- that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- that the Greene's network and internet infrastructure is as secure as possible
- that Greene's meets any OSCB e- safety guidance that may apply
- that Greene's networks and devices are password protected
- receives reports of e-safety incidents and creates a log of incidents

The College Principal, as designated safeguarding lead, should be trained in e-safety issues and be aware of the potential for safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Staff and tutors are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Greene's e-safety policy and practices
- they report any suspected misuse or problem to the Academic Registrar for investigation, action and possible sanction
- all digital communications with students and parents & guardians should be on a professional level
- e-safety issues are embedded in all tutoring, homework and other learning activities
- students understand and follow e-safety and acceptable internet use practice
- students have a good understanding of internet research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in tutorials and other school activities and implement current policies with regard to these devices

Students

- are responsible for using the internet in accordance with current Greene's e-safety policy and recognised safe internet practices
- have a good understanding of internet research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies away from Greene's premises and realise that this policy covers their actions away from Greene's premises, if related to Greene's.
- should understand the potential short-term and long-term consequences of internet malpractice and unacceptable use.

Parents & guardians play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way and are encouraged to support Greene's in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to Greene's Online
- their children's personal devices – especially mobile phones – in Greene's

The Student Committee has responsibility for issues and student led initiatives regarding e-safety. It provides a consultative online safety forum that has representation from the student body and a nominated student online safety representative. The online safety representative of the student committee is responsible for regular reporting to the Academic Registrar. The online safety representative will assist the College Principal with:

- the annual review and regular monitoring of the Greene's E-Safety Policy; and
- consulting the student body about the provision for online safety.

Policy Statements

Education – students: Whilst regulation and technical solutions are very important, their use must be balanced with educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of Greene's e-safety provision.

Children and young people need the help and support of Greene's to recognise and avoid e-safety risks and build their resilience.

Staff should reinforce e-safety messages during tutorials and when setting homework that requires access to the internet. This includes access to messaging systems, internet notice boards, virtual learning environments (VLEs) and other internet based educational resource environments.

Key e-safety messages and understanding should be reinforced as part of each student's personal development programme.

Students are informed so as to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Students should also be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Training of staff: All staff receive appropriate e-safety training and understand their responsibilities, as outlined in this policy. All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand this e-safety policy.

Technical infrastructure and equipment: Greene's will ensure that the internet infrastructure is as safe and secure as is reasonably possible and that statements and procedures approved within this policy are implemented.

In particular, that:

- Greene's information technology systems are managed in ways that ensure that Greene's meets recommended technical requirements
- There are regular – at least once per year – reviews of the safety and security of Greene's technical systems
- Servers, wireless systems and cabling are secure and access restricted
- All users have clearly defined access rights to Greene's Online
- All users of Greene's Online are provided with a username and secure password and users are responsible for the security of their username and password.
- Software licence logs are accurate and up to date and that checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. owned by Greene's from accidental or malicious attempts which might threaten the security of systems and data. The college infrastructure and individual workstations are protected by up

to date anti-virus and anti-malware software.

Bring Your Own Device (BYOD)

The learning opportunities offered by technology are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the tutorial. This has led to students and tutors bringing their own devices to facilitate their learning. However, there are a number of e-safety considerations for BYOD that need to be born in mind.

Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations include: levels of secure access, filtering, data protection, storage and transfer of data, training, support and acceptable use. This list is not exhaustive.

- Greene's has a set of clear expectations and responsibilities for all users
- Greene's reserves the right to ask students to show the contents of their devices when on College premises
- Greene's adheres to the principles of the 2018 Data Protection Act
- Network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the Greene's normal filtering systems, while being used on the premises
- All users will use their Greene's Online username and password and keep this safe

Use of digital and video images

Staff, parents & guardians and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees. The college will inform and educate users about these risks to reduce the likelihood of the potential for harm.

In particular:

- When using digital images, staff and tutors should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Parents & guardians may take videos and digital images of their children at Greene's events for their own personal use – as such use is not covered by the Data Protection Act. To respect privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should comments on any activities involving other students in the digital and/or video images concerned be made.
- Staff may take digital and/or video images to support educational aims, but must follow Greene's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Greene's equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital and/or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or Greene's into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of individual students are published on the Greene's website.
- Student's work can only be published with the permission of the student and parents or guardians.

Data Protection: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. The Greene's Data Protection Policy Statement and Procedures should be referred to and followed.

Communications: A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Greene's currently considers the use of these technologies -

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to Greene's	X					X		
Use of mobile phones in lessons		X					X	
Use of mobile phones in social time	X				X			
Taking photos on mobile phones / cameras	X					X		
Use of other mobile devices e.g. tablets	X					X		
Use of personal email addresses at Greene's			X		X			
Use of messaging apps				X				X
Use of social media	X					X		
Use of blogs	X					X		

When using communication technologies the following is considered good practice:

- The official Greene's e-mail service may be regarded as safe and secure. Users should be aware that e-mail communications may be monitored.
- Users must immediately report, to the Academic Registrar, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents and guardians must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Greene's website and only official e-mail addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Greene's staff should ensure that:

- No reference should be made in social media to students, parents and guardians or staff and tutors
- They do not engage in online discussion on personal matters relating to members of the Greene's community
- Personal opinions should not be attributed to Greene's

Greene's use of social media for professional purposes is monitored.

Unsuitable / unacceptable activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned. Other activities e.g. cyber-bullying are also banned and could lead to criminal prosecution. There are a range of activities which may, in some other context, be legal but are unacceptable in the context of Greene's, because of the nature of our activities.

This policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using Greene's systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Greene's					X	
Infringing copyright					X	X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	X
Creating or propagating computer viruses or other harmful files					X	X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)				X		
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X	X		
File sharing		X				
Use of social media under approved circumstances			X			
Use of messaging apps under approved circumstances		X				
Use of video broadcasting e.g. You Tube for educational purposes		X				

Responding to incidents of misuse

The flow chart (below) should be referred to when deciding how to respond to online incidents of misuse.

Illegal Incidents: If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police – CEOP (Child Exploitation and Online Protection) Centre.

Other Incidents: It is hoped that all members of the Greene's community will be responsible users of digital technologies. However, there may be times when unacceptable behaviour could take place, through careless or irresponsible or, rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Inform the Academic Registrar.
- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to a report (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by OSCB
  - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police-CEOP immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour; the sending of obscene materials to a child; adult material which potentially breaches the Obscene Publications Act; criminally racist material; and other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for Greene's and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. A completed report should be retained for evidence and reference purposes.

Greene's Actions & Sanctions: It is more likely that the Greene's will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Greene's community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students **Actions / Sanctions**

Incidents:	Refer to Personal Tutor / tutor	Refer to Academic Registrar	Refer to College Principal	Refer to Police	Refer for action re filtering / security etc.	Inform parents and guardians	Removal of network / internet access rights	Warning	Further sanction e.g. suspension
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during tutorials	X	X			X			X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	
Unauthorised use of social media / messaging apps / personal e-mail	X	X						X	
Unauthorised downloading or uploading of files		X					X	X	
Allowing others to access Greene's network by sharing username and passwords		X	X				X	X	
Attempting to access or accessing the Greene's network using another student's account		X	X				X	X	
Attempting to access or accessing the Greene's network using a staff account		X	X				X	X	
Corrupting or destroying the data of other users			X			X	X	X	
Sending an e-mail, text or message regarded as offensive, harassment or of a bullying nature			X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions			X			X	X	X	X
Actions which could bring Greene's into disrepute or breach the integrity of Greene's			X			X	X	X	
Using proxy sites or other means to subvert the network filtering system			X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			X	
Deliberately accessing or trying to access offensive or pornographic material			X		X	X	X	X	
Receipt or transmission of material that infringes copyright or the Data Protection Act			X		X	X	X	X	

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to College Principal	Refer to OSCB	Refer to Police	Refer for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Unacceptable personal use of the internet/social media/personal e-mail	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access Greene's Online by sharing username and passwords or attempting to access or accessing the Greene's Online using another person's account		X				X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X			X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X				X	X
Using personal e-mail / social networking / instant messaging / text messaging to carry out digital communications with students		X				X		
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the Greene's into disrepute or breach the integrity of the ethos of the Greene's		X				X		
Using proxy sites or other means to subvert the Greene's filtering system		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X		X
Breaching copyright or licensing regulations		X				X		X
Continued infringements of the above, following previous warnings or sanctions			X	X	X		X	