Greatham primary school

Petersfield Road, Greatham, Nr Liss, Hants. GU33 6HA
Tel: 01420 538 224
Website: www.greathamschool.co.uk
E-Mail: info@greathamschool.co.uk

HEADTEACHER: Miss J Goman
ADMINISTRATION OFFICER: Mrs Morris

Policy Name:	E-Safety Policy
Date Published:	15 December 2014
Document Owner:	Charlie Addison
Signature of the Head Teacher	Joanna Goman
Review Cycle:	3 years
Next Review Date:	December 2017 December 2020 December 2023 December 2026
Notes	**E-safety is considered a high priority. Therefore, a governor has responsibility for e-safety and will undertake annual monitoring.**

The school adopts the Manual of Personnel Practice and this policy should be read in conjunction with the following policies:
Acceptable Use of ICT Policy
Code of Conduct Policy
Safeguarding Policy
Child Protection Policy
Behaviour Policy

Rationale

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

Aims of the Policy

Our primary aims and objectives with regard to internet safety are as follows:

1. To ensure the safety and well-being of our students while they are using the internet both within the school premises and at home.
2. To educate our students about the potential risks and responsible use of the internet.
3. To provide guidance to teachers and parents on internet safety.
4. To establish clear procedures for addressing internet safety incidents.
5. To continually review and update our internet safety practices to reflect the evolving nature of online technologies and threats.

Safeguarding

Throughout the PSHE curriculum pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Hampshire County Council can accept liability for any material accessed, or any consequences of Internet access.

What we will do?

It is critical that we focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching will always be age and developmentally appropriate.

We will:

Ensure that effective filtering, monitoring and firewall technologies are in place**.
Set clear boundaries with staff and pupils for the appropriate use of the internet and digital communications.
Always ensure that an adult is present when a child is on an internet device in school.
Educate pupils in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
Ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
Review the school computing system security termly and install and update virus protection.

The underpinning knowledge and behaviours that will be taught are:

How to evaluate what is seen on line - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

How to recognise techniques used for persuasion – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others e.g. online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation), techniques that companies use to persuade people to buy something.

How to behave appropriately online– This will enable pupils to understand what acceptable and unacceptable online behaviour look like. We will teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. We will teach pupils to recognise unacceptable behaviour in others.

How to identify online risks – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

How and when to seek support – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

What we expect children to do

1. Students are expected to use the internet in a responsible and respectful manner, following the guidelines provided in this policy.
2. They should not share personal information, such as their full name, address, phone number, or school details, with anyone they meet online.
3. Students must report any inappropriate or harmful online content or behaviour to a trusted adult, such as a teacher or parent.

What we expect parents to do

1. Parents and guardians are encouraged to be actively involved in their child's online activities and set appropriate limits on screen time.
2. They should educate their children about online safety and monitor their internet use at home.
3. Parents are urged to report any concerns or incidents related to internet safety to the school so that home and school can work in partnership.

Log-ins and Passwords

Pupils and staff must not disclose any password or login name to anyone or allow anyone else to use a personal account. Pupils and staff must not attempt to gain access to the school network or any internet resource by using someone else's account name or password. In order to assist with the smooth running of lessons class teachers will be aware of their pupil's login details in case the pupils forget them.

Remote learning and Learning Platform

Greatham Primary School uses Google Apps for Education and Purple Mash as VLEs. All pupils have access to the VLEs to create, store and update their learning. All pupils are given a login name and passwords to enable safe access in school and at home.

It may be necessary and appropriate for some lessons to take place on line. These will be undertaken using the VLEs. Parents will always be informed prior to a session taking place and children and staff must both be in suitable locations where there is nothing happening in the background. Children and staff must be appropriately clothed and where possible, parents should be present/ able to hear. Children who are unable to access this form of learning will be identified and supported appropriately.

E-mail- for pupils and staff with school email addresses

School staff will be provided with a login where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to perform their role.

Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided.

Staff accessing email must set devices to lock when they are away from them. All staff should make sure that they have a PIN or passcode on any mobile device where they access their school email. This is to ensure no personal data or images can be accessed from mobile phone or a device if it is lost, stolen, or accessed by pupils.

Pupils in KS2 will receive a login for Google Classroom in the form of an email address. This platform enables them to access all of the Google Education suite of apps. Children must report if they receive offensive or inappropriate messages. Pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from their parents. The forwarding of chain letters is not permitted. Children are taught this.

Use of IT including social media
Internal e-mail and internet systems must be used only in accordance with the school's acceptable use of ICT policy which is located in the school office.

School staff must take care to protect their privacy and protect themselves from risk of allegations in relation to inappropriate relationships and cyberbullying. Staff must not have any unauthorised contact or accept 'friend' requests through social media with any pupil (including former pupils and/or those who attend other schools) unless they are family members. Staff must exercise caution when having contact online through social media with parents so as not to compromise the school's reputation or school information.

Please refer to the school's acceptable use of ICT policy (located in the school office) for further guidance on acceptable and unacceptable use of IT, social media and mobile phones. Staff may also refer to the school's leaflet '[Use of ICT Resources Do's and Don'ts: advice for school staff]' (located in the school office).

Mobile Devices
If pupils bring mobile devices to school then they must be placed in their school bag at the start of the day and remain there until home time. School cannot be held responsible for the safety of these devices and they are brought at pupil's own risks. Any pupil who is seen with a mobile device during the school day will have their phone removed. Pupils may not make personal calls from a mobile phone during the school day. Mobile phones may not be used to take pictures or videos of pupils and staff. Pupils should not send/receive email or text messages to/from their mobile device during the school day. Any inappropriate use of mobile devices such as cyber bullying must be reported to the Head teacher or DSLs. Staff should only use their mobile phones at appropriate times of the day, during the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

Authorising Internet access
All staff must read and sign the 'Staff Acceptable Use Policy and Code of Conduct for ICT' and 'School Social Media Policy' before using any school ICT resource, including any laptop issued for professional use.

Published content and the school web site
Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The Head Teacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students' images and work
Photographs that include pupils will be selected carefully so that images of individual pupils cannot be misused. Pupils' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs. Written permission, using the approved permission form, from parents or carers will be obtained before photographs of pupils are published on the school web site.

Internet filtering and monitoring
If staff or pupils discover an unsuitable site, it must be reported to the Head Teacher or another member of the SLT. We will implement appropriate internet filtering and monitoring systems to block access to inappropriate content and to ensure that students are using the internet safely while at school. Filtering reports will be checked regularly by the headteacher and acted upon to ensure compliance with this policy.

No internet filtering is 100% effective and on accidentally discovering material that makes them feel uncomfortable we instruct students to:

- Switch off their screen, place their tablet face down or close their laptop straight away without showing their neighbours
- Tell a teacher or member of staff straight away

Incident Reporting and Response
Any incidents related to internet safety will be taken seriously and addressed promptly. Our response may include:

1. Investigating the incident.
2. Involving parents/guardians and, if necessary, the appropriate authorities.
3. Implementing appropriate consequences for students involved in harmful online behaviour.
4. Offering support and guidance to victims of online harassment or bullying.

Managing emerging technologies
Emerging technologies will be examined for educational benefit. Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. The use by students of cameras in mobile phones will not be acceptable unless they have the permission of the Head Teacher. It should be noted that games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering.

Protecting personal data
The school is committed to maintaining the principles and duties in the GDPR at all times. This means that we ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure. Actions taken include:
Secure access across the school's private network (provided by Agile IT) which includes centrally managed firewalling, email and content filtering and Virus Protection
Password protected computers which automatically 'lock' when not in use
Regularly changed passwords
Use of work email secure line addresses only

Handling e-safety complaints
Any complaint about staff misuse must be referred to the Head Teacher and if the misuse is by the Head Teacher it must be referred to the Chair of Governors in line with the complaints policy (available on the school website). A hard copy of our complaints policy is available upon request.

Communicating e-Safety - Introducing the e-safety policy to pupils
E-Safety rules will be shared with all pupils before they access the internet. Each year, there will also be a dedicated week to raise the profile of internet safety.

The school's social media guidelines for pupils (listed below) will be shared and discussed with the class teacher at least every year during Internet Safety Week.

Contact details for social network sites	
The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools. http://www.saferinternet.org.uk/	Useful links
Facebook	Read Facebook's rules, report to Facebook, http://en-gb.facebook.com/help/181495968648557/
Instagram	Read Instagram's rules, Instagram Safety Centre, report to Instantgram https://help.instagram.com/

Kik Messenger	Read Kik's rules, Kik Help Centre, report to Kik https://kikinteractive.zendesk.com/anonymous_requests/new
Snapchat	Read Snapchat rules, read Snapchat's safety tips for parents, report to Snapchat https://support.snapchat.com/ca/abuse
Tumblr	Read Tumblr's rules, report to Tumblr https://www.tumblr.com/help
Twitter	Read Twitter's rules, report to Twitter https://support.twitter.com/
Vine	Read Vine's rules, report to Vine https://support.twitter.com/forms/vine
YouTube	Read YouTube's rules, YouTube Safety Centre, report to YouTube https://www.youtube.com/t/contact_us

Guidelines for Internet Use

- Do not engage in any abusive, threatening, unkind or bullying behaviour.
- Under no circumstances should negative comments be made about other pupils, staff or parents.
- Your online behaviour should be respectful of the opinions of others in your posts or comments.
- Users should not take credit for things they did create themselves, or misrepresent themselves as an author or creator of something found online.
- Research conducted via the internet should be appropriately cited, giving credit to the original author.
- The whole school community should understand that any form of cyber bullying to a pupil, parent or member of staff that is witnessed should be reported to a member of staff at the first possible convenience as it will not be tolerated. If it is possible to take a screen shot of the material this would aid the school to deal with the matter promptly.

** Email filtering list:

Not exhaustive and always improving in line with latest research.

duckduckgo.com
*.orteil.dashnet.org/cookieclicker/
*.emulatorgames.net/
*.romsgames.net/
*.vimm.net/
*.fullblackscreen.com/
*.yougottrolled.my.canva.site/
*.1v1.lol
*.CrazyGames.com
*.sites.google.com/site/unblockedgamessms6969/
*.game.fm/
*.sites.google.com/view/unblockedgameswtf2/
*.raaqa.com/drift-hunters/
bald.*-basics
.geforce-now/
fivenightsatfreddys.io
tiktok.com
www.dailystar.co.uk
www.thesun.co.uk
www.thesun.ie
kbh.games
kbhgames.com
miniplay.com
roblox.com

minecraft.net
sencoleader.pro
youtubekids.com
minecraft.net
poki.com
crazygames.com
orteil.dashnet.org