E-safety Policy

This policy covers all pupils in the school, including those in the Pre Prep department.

Keeping children safe in education (KCSIE 2021) is statutory guidance that schools and colleges in England must have regard to when carrying out their duties to safeguard and promote the welfare of children which includes safeguarding children online. Safeguarding and promoting the online welfare of children is everyone's responsibility.

This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying, data handling and the use of images** and is

Using this policy

- The person responsible for overseeing E-Safety at Greenfield is Peter Lovejoy, Head of Computing and Beth Reeve, Assistant Head & DSL.
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The e-safety policy is to be revised annually or when changes in legislation are released.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.
- The e-safety policy acknowledges the Home Office/DFE document 'How Social Media is Used to Encourage Travel to Syria and Iraq Briefing Note to School' and 'Teaching Online Safety in School' June 2019 and Keeping Children Safe in Education 2021.
- The e-safety policy is covered across the curriculum where appropriate, although predominantly through Computing, PSHE/RSHE and assemblies.

Managing access and security

The school provides managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school uses a recognised internet service provider- at present BT Internet.
- The school has an internet filtering system provided by Lightspeed systems. This form of filtering travels with the school devices enabling monitoring and protection away from school. We are also able to block any sites which may encourage radicalisation. This will be regularly checked to ensure that it is working, effective and reasonable.
- The school ensures that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by **personal** passwords.
- Use of the internet can be monitored and a log of any incidents kept to help to identify patterns of behaviour and to inform E-safety policy.
- The security of school IT systems are reviewed regularly.
- All staff that manage filtering systems or monitor IT use are supervised by senior leadership and have clear procedures for reporting issues.
- The school ensures that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

The school provides an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families takes place using school equipment and/or school accounts.

Pupils are advised not to give out personal details or information which may identify them or their location

Learning to evaluate internet content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news");
- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

E-Safety Policy

E-mail

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- At present pupils do not use email, although each does have an email address.

Published content e.g. school web site, school social media accounts

- The contact details are the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The website manager has overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission is obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.

Use of social media

- The school has a separate social media policy**.** The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype and Zoom is monitored by staff. Pupils do not use this without full supervision by a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the e-safety policy and staff code of conduct.
- Use of personal devices is clarified in the Staff Handbook and Code of Conduct.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school maintains a current record of all staff and pupils who are granted access to school IT systems.

E-Safety Policy

- At EYFS & Key Stage 1, access to the internet is by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet is with teacher permission with increasing levels of autonomy.
- People not employed by the school must read the Guest AUP before being given access to the internet via school equipment.
- Parents are asked to sign and return a consent form to allow use of technology by their pupil.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection/safeguarding procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's Behaviour Policy.

Cyberbullying

- Cyberbullying, as with any other form of bullying, is taken very seriously and is a form of peer on peer abuse (see KCSIE, 2021 for details). The anonymity that can come with using the internet can sometimes make people safe to say and do things that they would otherwise would not do in person. It is made clear to all members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

- Any incidents of cyberbullying will be dealt with in accordance with the school's Behaviour Policy, Anti-Bullying Policy and, where appropriate, the school's Safeguarding and Child Protection policies and procedures, regardless if this took place in or outside of school.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have read the guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

To pupils

E-Safety Policy

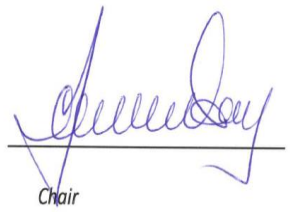
- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet. All children sign the AUP (appendix 1), which is then displayed in their classrooms.
- Pupils will be reminded about the contents of the AUP as part of their e-safety education.
- Pupils receive assemblies and lessons based on e-safety.

To staff

- All staff are shown where to access the e-safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff receive e-safety training as part of their safeguarding training.

To parents

- The school asks all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters and on the school web site.
- Parents are regularly reminded of e-safety issues through our newsletter.



Signed Chair of the Board of Governors

Reviewed September 2021

To be reviewed September 2022

Appendix 1 – Children's AUP

E-Safety Acceptable Use Policy

Year …

- I ask permission before using any laptop, computer or iPad
- I ask an adult which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe and if I am unsure then I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up then I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

Signature