e-safety at Greenside.

Curriculum.

Teaching during computing lessons in the first half term for every year group is focused on e-safety.

In Year 1, children learn:

- to understand what the internet is
- to compare how staying safe online is similar to staying safe in the real world
- to understand the rules for staying safe online
- to understand that information is private and should not be given out online
- to create effective usernames and protect their private information
- how to send and receive emails in a role-play scenario

In Year 2, children learn:

- to know that being safe online is similar to being safe in real life
- to recognise websites that are good for them to visit
- to understand that they should ask an adult they trust before visiting a particular website
- that the information they put online leaves a digital footprint (trail)
- what information is appropriate to be put online
- to analyse online behaviours that could be considered cyberbullying
- to know how to deal with a cyberbullying situation
- to recognise the importance of engaging a trusted adult when they experience cyberbullying

In Year 3, children learn:

- to understand the function of passwords
- to identify strategies for creating and protecting secure passwords
- how to create their own secure passwords
- how to compare and contrast how they are connected to different people and places, in person and on the internet
- understand how people can connect on the internet
- that the main purpose of product site is to encourage viewers to buy products
- how to recognise the importance of 'tone' in online communications
- the rules for writing clear and respectful emails

In Year 4, children learn:

- how to reflect upon their offline responsibilities
- how to examine their online responsibilities
- that good digital citizens are responsible and respectful in the digital world
- the benefits of sharing information online, but also about the safety and security risks of sharing certain types of information
- understand what type of information can put them at risk for identity theft and other scams
- how to distinguish between personal information, which is safe to share online, and private information, which is unsafe to share
- how to judge what it means to cross the line from harmless to harmful communication online
- to generate solutions for dealing with cyberbullying

In Year 5, children learn:

- how to identify the characteristics of strong password and create their own
- to establish expectations and norms related to appropriate online behaviour
- to participate responsibly and respectfully in an online community
- how to define what spam is
- to explore strategies for safely managing unwanted messages
- to identify different forms of spam
- that photographs can be digitally altered and consider the upside and downside of this practice
- how to understand that advertising uses photo alteration to help sell products.

In Year 6, children learn:

- how to compare and contrast online-only friends and in-person, face-to-face pals
- why important information should not be given to anyone without the permission of a trusted adult
- how to respond if an online-only friend asks them personal questions
- to compare and contrast their responsibilities to their offline and online communities
- to identify the characteristics that make someone an upstanding citizen
- to devise resolutions to digital dilemmas
- which information they should avoid sharing online because it is private
- which websites have privacy policies and why
- how to practise checking websites they visit for privacy policies and privacy seals of approvals
- how to empathise with targets of cyberbullying

- to recognise some of the key similarities and differences between in-person bullying and cyberbullying
- to identify strategies for dealing responsibly with cyberbullying
- how to evaluate online media messages that convey gender stereotypes
- to reflect why gender stereotypes sometimes can be limiting

To support the teaching and learning around e-safety, a number of resources are used including the BBC, Purple Mash, espresso, commonsense.org, internetmatters.org and NSPCC amongst others.

Parents

A number of approaches are used to inform and involve parents with e-safety. The NSPCC 'a parents' guide to being share aware' is sent home at the end of the Autumn term (in time for Christmas and any new technology that the children may receive) and in July as a reminder for over the summer months.

There are also links on the school website to the safer internet website and a guide for parents.

To coincide with 'Safer Internet Day', a parent workshop is held. Last year, the 'Operation Phoenix' team, from the child exploitation section of GMP also attended to advise parents and offer support.

Whole School

Safer Internet Day is taught each year where the children take part in a number of internet safety tasks and activities.

This year, to further enhance Safer Internet Day, we will be inviting Altru drama productions to school where they will perform the production of 'The

Tangled Web'. After the productions, a number of workshops and Q&A sessions will be held.

Regular assemblies, both whole school and class take place regularly. In these, the children explore what it means to be safe online and solve scenarios where things have not gone well.

<u>Security</u>

All staff laptops are encrypted to keep all data secure.

All staff laptops require a password as well as a username to log on to the server.

At present, we use Fortinet as our web filtering system. We are currently undergoing the process of changing supplier to use Smoothwall. This software is a market leader in web filtering systems.

Only school devices are allowed access to the server and WiFi.