E-Safety Curriculum 2018 Overview

Our E-Safety Curriculum is organised around 5 areas. It is based on the needs of our pupils, surveys of parents and Google's 'Be Internet Legends' programme.

Sharp: Think before you share (Be Internet Sharp)
Alert: Check It's For Real (Be Internet Alert)
Secure: Protect Your Stuff (Be Internet Secure)
Kind: Respect Each Other (Be Internet Kind)
Brave: When In Doubt Discuss (Be Internet Brave)

Year Group	Key questions	Skills
EYFS	What do we use computers for? What do you enjoy doing on the computer? What do we do if we see something that makes us feel uncomfortable?	**Sharp:** ▪ N/A **Alert:** ▪ Children begin to understand the differences between real and online experiences. **Secure:** ▪ Don't talk to strangers online. **Kind:** ▪ Be kind when playing games with others. ▪ Consider the consequences of their words and actions for themselves and others. ▪ Role play what to do when someone says or does something cruel or hurtful. **Brave**: ▪ What to do if they see something inappropriate on a website e.g. tell a trusted adult.

Year 1	What do we use computers for? What is the different between the computers and iPads? What do you enjoy doing on the computer? What is a pop-up? What do we do if we see something that makes us feel uncomfortable?	**Sharp:** ▪ Know how and why we keep passwords private. **Alert:** ▪ Are able to navigate age appropriate websites and know what to do when there are pop-ups. ▪ Know not everything they see on the internet is true. **Secure:** ▪ Learn when it is OK to share a picture e.g. Family day out. **Kind:** • Understand that the internet can be used to communicate with other people. • Role play how to behave in the online world, building positive and healthy online relationships. **Brave:** ▪ Know what to do if they find something inappropriate online. ▪ Know how to minimise a screen if they see something inappropriate on a website, and tell a trusted adult.

Year 2	What do we use computers for? What do you enjoy doing on a computer or iPad? Is it different at home and school? Why? What is personal information? What do we do if we see something that makes us feel uncomfortable? What is cyber bullying? What is a link? What is an advertisement?	**Sharp:** - Know what personal information is and why not to give it out. - Begin to publish appropriate information on blogs which includes text and pictures. (not photographs) **Alert:** - Know that not everything on the internet is true. - Learn how websites encourage users to click on links. **Secure:** - Know how to set and keep passwords secure. - Know what privacy settings are. **Kind:** - Role play how to behave in the online world, developing and sharing strategies for dealing with cyber bulling. - What might an unhealthy relationship online look like? E.g. telling a child to privately message, not tell friends or family. - Know that some video games are inappropriate and why there are age labels on games. **Brave:** - Know what to do if you are unhappy about any aspect of the internet. - Know how to make a screen shot to save evidence of cyber bullying. - Know how to report unpleasantness online.

| Year 3 | Can you just take any picture and use it? Should you give your real name online? Real address? What situations would people ask you for your real name? What is a 'scam'? Can you trust all the information you see / find out on the internet? What is 'fake news'? What can we do if we are bullied in the online world? Why are some games labelled as being for older children? | **Sharp:**
• Begin to use e/mail, instant messaging, and blogs to exchange ideas with other learners within school.
• Protecting my digital footprint – what should and should not be shared online.
• Understand that they may unwittingly provide personal information, e.g. by webcam and how to prevent this.
Alert:
▪ Attempt to distinguish between fact/fiction and opinions.
▪ Investigate what 'fake news' is.
▪ Know that pop ups can happen and know what to do.
▪ Be aware of 'phishing' and some online 'scams'.
Secure:
▪ Know how to set secure passwords and keep them secure.
▪ Know what privacy settings are and the need to review them regularly.
▪ Know that you can't win a competition that you have not entered.
▪ Learn that if something is 'free' online then your information may be the cost.
▪ Understand that a 'free' game may have 'in game' purchases and that these need permission from parents.
Kind:
▪ Know what cyberbullying is and what to do about it.
▪ Learn how to resist peer pressure to play age inappropriate games through role play.
▪ Describe how to respond to hurtful online behaviour in ways that keeps them safe and healthy.
▪ What might an unhealthy relationship online look like? E.g. telling a child to privately message, not tell friends or family, asking a child to keep secrets.
Brave:
▪ Know who they should tell when they are uncomfortable.
▪ Know how to report unpleasantness online and how to block people from contacting them.
▪ Know that it is not safe to meet anyone whom they have only talked to online and do not know in the real world, without a trusted adult.
▪ Know that some video games are inappropriate and why. |

| **Year 4** | How would you respond to online bullying? What would you do with a text message you don't like or that makes you feel uncomfortable? How do use blogs? What sort of comments should you leave? What do you do if someone leaves a comment that makes you feel bad? How can you find the author of a document or website? | **Sharp:**

• Use a range of online communication tools to exchange information and collaborate with others beyond school. This may include e mail, instant messaging, social networking, online gaming, mobile phones. Children should be able to explain how you to keep themselves safe.

• Learn to make choices about which image and video material (including games) are suitable for their age and experience.

• Learn ways they can start to build a positive digital footprint.

• Understand that they may unwittingly provide personal information, e.g. by webcam

Alert:

▪ Learn why they should never open e-mails or messages from unknown sources and why attachments can be dangerous to their safety online.

▪ Be aware of ways to spot a 'scam' and know what to do if they spot one.

▪ Know that not everything on the internet is true and what to do if they access something inappropriate.

▪ Be able to talk about what 'fake news' is and how to spot it.

Secure:

▪ Know how to access privacy settings, review them regularly and why they are needed.

▪ Investigate games / social media which are free and discuss how these companies make money.

▪ Learn that if something is 'free' online then your information may be the cost.

▪ Create and keep secure passwords of increasing complexity and strength.

Kind:

▪ Know what cyberbullying is and be able to talk about their strategies to avoid it and what to do about it when it does happen. Learn how to resist peer pressure to play age inappropriate games through role play.

▪ Describe how to respond to hurtful online behaviour in ways that keeps them safe and healthy.

▪ What might an unhealthy relationship online look like? E.g. telling a child to privately message, not tell friends or family, asking a child to keep secrets.

Brave:

▪ Know who they should tell when they are uncomfortable; always talk to someone.

▪ Know that it is not safe to meet anyone whom they have only talked to online and do not know in the real world, without a trusted adult.

▪ Know how to take a screen shot of messages for evidence, report unpleasantness and block others. |

| Year 5 | When do you meet people online? When do you give your real name? Would you create a whole new online persona? Why would people not keep their real name online? Why do some websites have age restrictions? Is it wrong to break the rules to be a member? What does it mean to lie about your age for sites such as Facebook or Snapchat? How do you respond to blog posts? What happens if someone leaves a comment that makes you feel bad? What should you do? | **Sharp:**
■ Understand the difference between 'public' and 'private' in the online world.
■ Understand the consequences of sharing your location.
■ Explain the types of information which should not be publicly shared, including images.
■ Understand the potential risks of providing personal information in an increasing range of online technologies, particularly social networking and gaming.
■ Know that information is gathered from photographs as well as what is written in text.
■ Evaluate their own use of web publishing tools and how they present themselves online, including images and the use of a webcam.
■ What to do if they have shared something they realise they should not have done.
Alert:
■ Recognise that some information on the internet can be untrue e.g. 'fake news' or biased (advertising).
■ Develop strategies for identifying the origin of websites.
■ Talk about how to identify 'scams' and what to do.
■ Be aware that people may not create honest profiles of themselves.
Secure:
■ Know how to access privacy settings, review them regularly and use other safety tools online.
■ Investigate games / social media which are free and discuss how these companies make money.
■ Create and keep secure passwords of increasing complexity and strength.
■ Learn to identify and protect themselves from 'scams'.
■ What to do if an online account has been compromised.
Kind:
■ Understand why they should respect the privacy of others, taking care of personal information and images shared with them.
■ Learn through role play how to behave when using social media.
■ Understand that information needs to be processed and interpreted for others, not just copied. They understand the term plagiarism.
Brave:
■ Know who they should tell when they are uncomfortable.
■ Understand that malicious adults use the internet to make contact, and groom young children and how to report any suspicions.
■ Explain why it is not safe to meet anyone whom they have only talked to online and do not know in the real world, without a trusted adult. |

| Year 6 | When do you meet people online? When do you give your real name? Would you create a whole new online persona? Why would people not keep their real name online? Why do some websites have age restrictions? Is it wrong to break the rules to be a member? What does it mean to lie about your age for sites such as Facebook or Snapchat? How do you respond to blog posts? What happens if someone leaves a comment that makes you feel bad? What should you do? | **For all areas use the games within g.co/interland**
Sharp:
Understand the difference between 'public' and 'private' in the online world.
Understand the consequences of sharing your location.
Explain the types of information which should not be publically shared, including images.
Understand the potential risks of providing personal information in an increasing range of online technologies, particularly social networking and gaming.
Know that information is gathered from photographs as well as what is written in text.
Evaluate their own use of web publishing tools and how they present themselves online, including images and the use of webcam.
Evaluate how others would see them from their digital footprint.
Talk about how they can create a positive digital footprint.
What to do if they have shared something they realise they wish they had not done.
Alert:
Recognise that some information on the internet can be untrue e.g. 'fake news' or biased (advertising).
Develop strategies for identifying the origin of websites.
Identify different types of online scams aimed at young people and know where to go for help.
Be aware that people may not create honest profiles of themselves.
Use a range of sources to check validity and recognise different viewpoints. Critically evaluate the information they use and understand some of the potential dangers of not doing so.
Secure:
Investigate games / social media which are free and discuss how these companies make money.
Create and keep secure passwords of increasing complexity and strength.
Learn to identify and protect themselves from 'scams' e.g. competitions they have 'won' and offers that seem too good to be true.
Understand the pitfalls of your social networking sit being linked from a friend's site.
How to avoid being 'tagged' on social media.
The need for regularly reviewing your privacy settings on social media.
What to do if an online account has been compromised.
Kind: Understand the severity of the impact on an individual of sending or uploading unkind or inappropriate content, particularly when a wider audience views the content. Understand that you should not publish other people's pictures or tag them without their permission. |

		- Understand why they should respect the privacy of others, taking care of personal information and images shared with them. - Understand what cyberbullying is and can explain clearly what to do if it happens to them. - Be aware of the issues of plagiarism, copyright and data protection in relation to their work, understanding that the resources they find may be covered by copyright. **Brave:** - Know who they should tell when they are uncomfortable. - Understand that malicious adults use the internet to make contact, and groom young children and how to report any suspicions. - Explain why it is not safe to meet anyone whom they have only talked to online and do not know in the real world, without a trusted adult.