LAKESIDE PRIMARY ACADEMY

The Rose Learning Trust

Whole school progression in Online Safety

Term	Year one/two	Year three	Year four	Year five	Year six
Autumn term 1	**People Online** This lesson explores friendship and trust and how it takes time to make judgements about new people we meet. It introduces the concepts of being online, and some of the ways that it is possible to connect and communicate with others online.	**People Online - Friend of a friend** Due to the physical distance, children may not be as cautious interacting with new people as they would be in real life. They need to understand the risks of talking to new people online: they may not be who they say they are, they may lie, and they may try to trick.	**Digital Footprint** The lesson introduces the concept of a Digital Footprint. Students will learn that their Digital Footprint is made up of all of their traceable online activity including their personal profiles, comments, website searches, website visits, blogging, vlogging, videos and photos that they look at and post online. All of these activities leave a permanent digital trail rather like leaving a trail of footprints	**Digital Footprint** This lesson explores the use of privacy settings and the care needed when creating online profiles to reduce the amount of information revealed in our digital footprint. It focuses on the different ways people are able to communicate with each other online and the steps we can take to reduce contact from new people online.	**Safe Sharing** The first scenario in Gooseberry City is designed to help learners to think critically about how they share online. Any information that is shared online can be saved as a screen shot, copied or shared further by the recipient and can be held indefinitely (even if the original sharer deletes it). Images can be changed, commented on or falsified by other users. If transmitted over insecure connections, data may be hacked for fraudulent or other purposes.

Autumn term 2	**Personal Information** This lesson introduces the concept of personal information, where it might be found online, why it is important to protect it online and how to do so.	**Perfect Passwords** This lesson provides opportunities for children to think about what passwords are used for and how to create strong passwords.	**Click Jacking** The focus of this lesson is to educate learners about the security risks of engaging with online clickjacking/Clickbait. They will learn that Clickjacking is a security threat which uses a range of tactics including images and persuasive language to entice the user and tricks them into clicking a webpage which is disguised as something else. This can lead to unknowingly sharing personal information with a fraudster.	**Junk Email** Junk email (also known as spam) is unsolicited electronic mail sent via the internet, usually in bulk to many users at once. Some junk email is harmless advertising, but some are scams, harbouring malware or attempts to hack personal information. In the UK it is illegal to send unsolicited marketing emails to individuals (and it can be reported to the ICO) however, lots of spam comes from outside the UK.	**Digital Footprint** This scenario explores issues surrounding the use of technology and digital media focussing on the pressures to share online, the potential impact on reputation of thoughtless sharing and the difficulty of removing content once shared. In seeking popularity, young people can feel pressured to over share or push the boundaries of what is acceptable by creating and sharing content that encourages others to ‘like’, ‘share’ or ‘forward’ it. This may include content that demeans, ridicules and offends people.
	Perfect Passwords This lesson introduces the concept of a password and the definitions of “characters” and “symbols”. It explores where and why passwords are used, and how to create passwords that are strong and secure.	**Staying Private Online** Children will be encouraged to think critically about the permissions sought and to be wary of those that don’t make sense. As they are still young, the main purpose is to raise awareness and to encourage them to seek adult help before downloading apps or granting permissions.	**Webcam Wise** Because children have access to a wide range of devices and apps, it is important to educate them in how to stay safe whilst online, rather than preventing them from using it. Children are also encouraged to consider the nature of friendship, and with whom and how they interact whilst online, thus reducing the risk of engaging with unwanted contact but also recognising when it is going wrong. They should also consider that just because they know someone, does not mean they should communicate online with them	**Location Sharing** Online games that encourage players to use their devices outdoors can have positive benefits to health, wellbeing, and developing independence. These types of games may need “location settings” to be turned on in order to play and this can facilitate contact from others nearby. This lesson encourages learners to assess the positives and negatives of location sharing and to develop strategies for safe gaming outdoors.	**Receiving Images** This lesson explores the types of media that might put learners at risk, and the importance of thinking carefully about what and with whom they share things online. It addresses the consequences of sharing rude images as well as the law and how to respond to and report inappropriate messages. Clearly inappropriate content should never be shared with others, but a copy of the message, sender, date and time should be kept briefly, as proof.

LAKESIDE
PRIMARY ACADEMY

The Rose Learning Trust

Spring term 1	**Fake Profiles** It focusses on recognising what online profiles are, how they are created, where they might be found and the sort of information they might contain. It encourages children to be sceptical about the truth of online profiles, and to be cautious when interacting with people online, both at the point of contact and as a relationship develops	**Safe Sharing** It's important to make it clear to children, even at this age, that once something is online, it's hard to remove it. Don't, say it's impossible	**Safe Sharing** Children will be encouraged to explore the differences between on and offline communications, between banter and bullying and how to reduce the risk of unintentional upset. They will look at reducing the risks of bullying by being careful what they share. They will explore how to respond to bullying and how to support a friend.	**Extreme Promises** The scenario explores the difference between facts, opinions and beliefs and encourages reflection about feelings and about people's motives. It aims to encourage a healthy scepticism of unsolicited offers, emotionally persuasive offers (including threatening messages) unlikely promises and a questioning attitude, before making important decisions. It empowers children to resist persuasive or extreme promises.	**Real Time Sharing** This lesson acknowledges the benefits of technology when out and about but also addresses the risks and encourages a discussion of the pressures that can lead to overuse, to the detriment of our well-being. It will remind learners not to overshare, to restrict the audience they share with and to resist the urge to share in real time. It also focuses on how online posts can be perceived differently or misinterpreted by others and encourages learners to consider the consequences of their actions
	Safe Selfies Taking and sharing 'selfies' is popular with people of all ages. Although it can be fun, selfies can also create risks, if they are shared with others online – by revealing personal information (such as name, school or location), by leaving someone vulnerable to bullying (through ridicule or teasing) or by damaging their digital footprint/reputation (with silly or rude poses)	**Location Sharing** This lesson provides an opportunity for children to learn more about how locational data is sometimes attached to media (especially photos and videos). They will explore why this can be a useful feature and also about the risks.	**Online Gaming** This lesson addresses the health and wellbeing risks of spending too much time online, the type of unpleasant behaviour that can occur in online gaming and the risks of contact with new people online while gaming. It can be difficult for children to know the intentions of the people they communicate and collaborate with online. It can also be confusing to think that there are some people online who may want to put them at risk, so it is important they know how to respond safely to the requests that they might make.	**Video Chats** The immediate and visual nature of video chatting means that children may not take time to consider the appropriateness of a request and be disinhibited. This lesson aims to alert children to persuasive techniques, how to resist them as well as the risks and the consequences. It teaches them that images can be saved, screenshot, altered and shared quickly and widely. It looks at the nature of blackmail and how an initial request can escalate into more demanding situations. It also addresses the difficulty and ways of seeking help when we have done something embarrassing.	**Grooming** In this lesson they will be encouraged to explore how friendships are formed, how information posted online can reveal information about us and how this can be exploited by groomers to gain a child's trust. Although it can be difficult to spot, there are some warning signs of grooming, not least an intuition that something is not quite right. The lesson will focus on recognising these signs and knowing how to respond safely as well as reducing the risk of contact in the first place.

Spring term 2	**Share Safely** This lesson explores the impact on others of sharing their images online, the loss of control once an image is shared online and the capacity of others to alter and misuse online images. It focuses on the need to be kind and considerate of others when sharing online. It also introduces the concept of copyright in photos and other work that may be created by learners or seen online.	**Online Gaming** Online games raise issues in three main areas of risk: Content – exposure to inappropriate material, both visual and audio (violence, swearing or sexual), Contact – online interaction with other users, including groomers, (particularly via chatrooms and real-time messaging capabilities), Conduct – bullying, abuse, players (griefers) who intentionally stir up trouble or harass other players, unfair game play (cheats), pressure to make in-app purchases, risk of revealing personal information, risk of addiction or excessive play time and risk to reputation.	**Boundaries** This lesson offers opportunities for learners to discuss safe practices while online and offers some suggestions on how to respond if they come in contact with inappropriate material	**Online Bullying** Bullying takes many different forms online and it can be particularly pervasive due to the ease of contact 24 hours a day and the ability to be anonymous. It can escalate quickly, and, if carried out in public forums (such as social media or online gaming) can be extremely devastating due to the wide audience and permanence of the record. It can have long lasting effects on the victim's confidence, self-esteem and mental health.	**Streaming, Downloading, Uploading** Learners will be encouraged to consider how to identify safe and legal online sites, and to be sceptical of free offers. They will also discuss the risks associated with live streaming their own original videos including exposing personal information about themselves or others or their location, receiving unkind comments, sharing too widely or losing control of how their content is onward shared and altered by others.
	Video Chat This lesson introduces video chatting via webcams or device cameras, which enable us to see as well as hear each other as we chat over the internet. Video chat enables cheap, personal contact to enhance communication in a wide variety of social and business situations.	**Online Bullying** In this lesson, children will reflect on the impact and consequences of online bullying and learn how to respond in a positive manner to similar situations they may face in the future.	**Illegal Downloads** This scenario deals with downloading and streaming music. Students may be familiar with this activity via reputable sites such as iTunes, Netflix etc and also on peer-to-peer file sharing networks. They may also have come across illegitimate sites offering free access to pirated content, with or without an awareness of the legality of this.	**Online Gaming** Learners are presented with opportunities to put into practice their knowledge of being a safe and responsible digital citizen. They are expected to consider all factors when making a choice and with support, decide on a positive and safe choice. They will develop critical thinking capabilities as they consider outcomes and take opportunities for peer collaboration to support discussions	**Passcodes and Passwords** The lesson also highlights the importance of ensuring devices are secure with people we know and trust by introducing the concepts of "disinhibition" and "banter". Learners will compare banter with bullying, recognising how one person's apparent playful teasing could be perceived as unkind or bullying.

Summer term 1	**Online Bullying** This lesson looks at online bullying, what constitutes bullying, what to do if you are bullied online and how to support someone else who is being bullied.	**Chatting Online** More and more, children are using technology to communicate with friends, so use this lesson to help them learn about the risks and benefits of chatting online. Help to develop their understanding of how to behave responsibly when communicating online, how to recognise and respond to online risks, and how to ask for help rather than trying to stop them from chatting online. Teach them that online chat isn't inherently risky, but that some people who use it are	**Downloading Apps** Although many apps and games are age restricted, the age verification processes can in many cases be easily avoided by giving a false date or year of birth or simply clicking to confirm a user is old enough. There is a difficult balance to strike between robust age verification requirements (now required for porn sites) and the need to provide details such as passport or other sensitive documents.	**Click Jacking** This may be to gain likes or information for marketing purposes or more seriously, leading to a Clickjack - a type of malware designed to trick us into clicking on something that is different from what we expect. This can download malware and learners will explore the impact that it can have on devices and users (virus, trojan, ransomware etc.) They will be made aware that while downloading a virus can be an inconvenience, the bigger issue is the compromise of security on devices and personal information. They will be encouraged to demonstrate an awareness of tempting click bait, the hidden risks of tempting links and the importance of responding to them safely.	**Sending Images** Sexting covers a range of communications, both text and images, ranging from flirty, mild innuendo to explicit and indecent. This lesson will focus mainly on images – photos and videos, (also known as youth produced sexual imagery), and primarily from the point of view of a young person who sends them
	Online Gaming This lesson will make children aware of the risks inherent in playing some online games, particularly those that involve communication, either text based or audio, via microphones and headsets. It will help them identify games which are age appropriate and teach strategies for reducing risk and responding	**Keeping Healthy** What are the risks for this age group? Excessive screen time means less time for physical exercise with consequent risks of obesity, short sightedness, heart and mental health issues. Taking phones to bed means children may be tempted to use them after bedtime or that they are disturbed by late night messaging, both of which can disrupt	**Images** As part of the lesson, ensure that children know from whom and how they can seek help with such issues within school, and the opportunities to seek confidential advice from services such as ChildLine. Be aware that some children may not realise that images, messages and videos could be deemed sexual or inappropriate and may not, therefore, create, view or share them with inappropriate	**Fake Profiles** This scenario encourages learners to reflect upon prior learning and raise awareness of the people that they may meet online. They should know that some people behave differently online than in real life, including by pretending to be someone they are not. An awareness of this, combined with knowing how to spot, question and respond to contact from new people online can protect them. We are familiar with the term 'Fake News'	**Keeping Healthy Online** Scenario 9 explores the positive and negative impact that technology can have on our health and wellbeing. It will examine the pressures to spend time online, the effects of excess screen time on both physical and mental wellbeing as well as strategies (including technological features) to manage it. See Teacher advice sheet.

	to any issues that might arise.	sleep, concentration, and affect their ability to learn.	intent. This may be as a result of youth, naivety or natural curiosity about bodies. They also may not recognise that the behaviour of others online is unsafe or inappropriate. Sexting refers to sexual messages (text or images) that are sent online, often via mobile phones but also via other connected devices. Messages can range from mild text innuendo to sexually explicit nude or semi-nude photos or videos. Children may send nudes as a dare, due to peer pressure, for the thrill of risk-taking, to gain "likes" or as a result of grooming or coercion. The issues arising from sexting include upset/harassment, reputational damage, bullying, breaking the law (potentially leading to a criminal record), grooming, blackmail and exploitation by sexual predators. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents involving children and young people complex.	and the various twists that media can place on a story they are covering. This is also true for online profiles. It is not always easy to spot a fake profile. It may be backed up by fake email addresses, social media accounts and online avatars. They are not always malicious, but they may be used for befriending, online grooming, identity theft and phishing (the fraudulent practice of gaining sensitive personal information through pretending to be a trustworthy source)	The minimum age for most social media is 13+ but many 11 and 12 year olds use it.

Summer term 2	**Searching** This lesson looks at the basics of searching for information online, using search engines and key words in the context of reviews for online games. It looks at how content is ranked and recognises that not all content online is reliable, suitable or safe	**Phishing** In this lesson, children learn about how scammers (fraudsters) use phishing techniques to try to get people to reveal their personal details, in order to commit fraud. They may simply request the information or tempt the recipient to click a link which either leads to a fake website, phone or email, or which downloads a virus to their computer. Children may be exposed to phishing via instant messaging (eg text, WhatsApp, SMS), email or by phone.	**Perfect Passwords** Through this lesson, students will consider the consequences of their actions and explore how to make a safe and morally right choice. This lesson offers opportunities to explore both the moral and legal issues of mis-using information and the prevalence of online identity theft. Learners will be guided with strategies to use if they are faced with a similar situation and given some support with creating strong passwords.	**Pop Up Messages** It explains that many online services are funded by advertising and this enables them to be free to use. It explores how and why our online activities might be tracked and analysed. This can lead to both targeted advertising or random pop-ups using persuasive language to try to influence our behaviour	**Video Chat** **Extreme Views** Learners will consider the potential risks that people met online may present and ways to reduce the chance of contact. The purpose is not to unduly worry them but to make them aware that online friends could be lying to them and that they should be sceptical. This lesson discusses “vulnerabilities” as well as the particular risks of video chat in the grooming process. It empowers learners to recognise signs of grooming, to resist inappropriate requests, to act when something doesn’t feel right and to know that it is not their fault.

Linking Online Safety to the National Curriculum

The national curriculum for computing aims to ensure that all pupils are responsible, competent, confident and creative users of information and communication technology …

KS1: Computing

- Recognise common uses of information technology beyond school
- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

KS2: Computing

- Understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact