E-Safety Policy

Date updated:	**September 2023**
Review date:	**30th September 2026**

Context

Firs Primary School recognises that there is a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their computing capability effectively and safely in their everyday lives.

The school is aware of its responsibilities in ensuring that technology usage within school is responsible, safe and secure.

This E-safety policy is written to reflect the importance of using technology safety and how by doing this, pupils and staff can be protected. The policy raises awareness of the safety issues by providing clear guidance on how to minimise risks and how to deal with any infringements of school policy. The policy also identifies how to introduce the concept of E-safety to pupils.

What is E-safety?

E-safety encompasses internet technologies and electronic communications. It highlights the need to educate pupils about the benefits and risks of using technology and how users can safeguard their online experience.

"E-safety may be described as the school's ability: to protect and educate pupils and staff in their technology" and "to have the appropriate mechanisms to intervene and support any incident where appropriate" *Ofsted, 2014.*

Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and outside of school by children include:

- The internet
- Smart phones
- Digital cameras
- E-mail
- Instant messaging
- Web cams
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Chat rooms
- Gaming sites
- Game consoles

We understand that the technological world is changed at great speeds and that "new opportunities, challenges and risks are appearing all the time,"

(Teaching Online Safety in Schools, DfE, 2019). We therefore recognise that "it is important to 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," ," (Teaching Online Safety in Schools, DfE, 2019).

Roles and Responsibilities

This policy is responsibility of the computing co-ordinator and Child Protection and Safeguarding Policy, Anti-Bullying Policy Mental-Health and Well-being Policy, Computing and PSHE Policy. The head teacher ensures that the policy is implemented and compliances with the policy will be monitored.

All teachers are responsible for promoting safe behaviours in their classrooms and following school procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bulling, abuse or inappropriate materials.

All staff should be familiar with the policy including:

- Safe use of e-mail;
- Safe use of the internet including social media;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobiles phones and digital cameras;
- Publication of pupil information/photographs and use of the website;
- Cyberbullying procedures
- Their role in providing E-Safety education for pupils.

The school includes E-Safety in their computing curriculum and ensure that every pupils has been educated about safe and responsible use. All classes teach e-safety discreetly for one half-term and revisit as necessary throughout the year.

"In the five schools where provision for e-safety was outstanding, all the staff, including members of the wider workforce, shared responsibility for it. Assemblies, tutorial time, personal, social, health and education lessons, and age appropriate curriculum for e-safety helped pupils to become safe and responsible users of new technologies" *Ofsted, 2014.*

Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies. Pupils' perceptions of the risks are not always mature and hence; e-safety rules are explained or discussed in an age appropriate manner. Children will also take part in 'Safer Internet Day.'

To teach E-safety the school uses the slogan 'Zip it, Flag it Block it' which is outlined clearly by Child Alert.

http://www.childalert.co.uk/article.php?articles_id=26

Other resources that teachers can use to support the teaching of E-safety:

http://www.kidsmart.org.uk/
https://www.thinkuknow.co.uk/
http://www.bbc.co.uk/cbbc/curations/stay-safe
Video Lee & Kim: https://docs.google.com/file/d/0B-xy4V542OOITEdsWWhEdlBqMDQ/view
Video Safer Internet Day: https://docs.google.com/file/d/0B-xy4V542OOIa0ZLaUtLaUtXU0k/view

Smart Crew: http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew

More information regarding our E-Safety curriculum can be found at the end of this policy.

How will the policy be discussed with staff?

Staff will be given a copy of the e-safety policy to review and any training in safe and responsible internet use can be provided when required. From November 2021 we have also subscribed to 'National Online Safety' where regular CPD can be assigned to staff to stay up to date with the latest information.

How will parents' support be enlisted?

Internet use in pupils' homes is an everyday activity. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet. In the school reception, a display highlights key apps that are popular amongst children and the harms and risks involved, as well as the age restrictions. All of the information has been accessed from https://www.net-aware.org.uk/ in conjunction with O2 and NSPCC.

From November 2021 we have also subscribed to 'National Online Safety' where parents can sign up to the school portal and receive informative training themselves and download guides linked to different elements of online safety. This will also be used as a tool in school to direct parents to if online safety incidents occur.

Any issues that have arisen within school which relates to internet usages will be handled sensitively by appropriate members of staff (class teacher, safeguarding lead, learning mentor, and/or headteacher) and parents will be advised accordingly. Any welfare concerns will be recorded and reported in line with the school's safeguarding policy. The e-safety policy will be also published onto the website.

How will complaints regarding E-Safety be handled?

The school will take all reasonable precautions to ensure E-safety. However owing to the international scaled and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or device. Neither the school nor the local authority can accept liability for material accessed, or any consequences of internet access.

Any complaint about staff misuses will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with the school safeguarding policy.

Complaints of cyberbullying are dealt with in accordance with our anti-bullying policy.

Managing the Internet Safely

The risks

The internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with restriction. These features of the internet make it both an invaluable resources used by millions of people every day as well as a potential risk to young and vulnerable people, as much of the material on the internet is published for an adult audience and some is unsuitable for pupils.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame' supportive culture if pupils are to report abuse.

Technical and Infrastructure

This school maintains a filtered internet connectivity which ensures that any websites that are inappropriate are blocked immediately. Both children and staff are aware that the internet is filtered and can be monitored and understand that they must report any failure of the filtering. If any material is suspected to be illegal the school will immediately refer this to the appropriate authorities.

Education and Training

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;

- Ensures pupils know what to do if they find inappropriate web material
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse
- Teaches E-safety as part of the computing curriculum (at the end of the document) in line with the National Curriculum

Managing Internet Access- Email

Email is now an essential means of communication for staff in our schools and increasingly for pupils and homes.

This school does not publish personal emails of staff on the school website. Staff must use only their provided school emails when signing up to websites and sending e-mails relating to school.

Pupils do not have access to a school email.

E-mails sent to external organisations should be written carefully.

Managing Internet Access- Digital Images

The headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

Photographs published on the school website / twitter account are only of those children who have had permission for this, and do not have full names attached.

Photographs taken by anyone in school are only taken by school equipment and can only be stored and accessed on schools devices.

Managing Equipment

The computer system/network is owned by the school and is made available to pupils to further their educations and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet or email activity on the network.

To ensure the network is used safely this school:

- Has set-up the network with a shared work area for pupils and a separate one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Pupils have access to their own class log in with set permissions.

Managing Internet Access- Social Media

Parents and teachers need to be aware that the internet has emerging spaces and social networks which allow individuals to publish unmediated content. Social networking sits can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. Pupils should be made aware of the age restrictions on the use of these websites and therefore schools should emphasise that the use of social media is inappropriate, but also be taught how accessible personal data can be and who it is shared to once it has been published.

School Social Media Accounts - Staff

YouTube

Firs Primary has a YouTube account linked to an unused email address within the school domain. The YouTube account can be accessed by any member of staff to upload videos to promote our school. One member of staff to take control of the account by being the recovery email. Before uploading videos to YouTube staff will inform parents in a written letter of their intentions and provide the opportunity for any parents to respond. Staff will also ensure that the only children to be shown in the videos are those with image publication consent. With the videos, no last names of the children will be published. All videos uploaded will be made public but the comments and ratings will be turned off.

Twitter

The aim of the school twitter account is to share learning experiences across the school and important information. The school twitter account will be linked to an unused email address within the school domain. The twitter account will be public to allow for re-tweets. The Twitter feed will also be published to the school website. The Twitter account can be accessed by any member of staff to upload examples of work, tweets about their memorable experiences etc. When sending tweets or publishing posts, staff will ensure that no last names of children will be published. One member of staff has control of the accounts by being the recovery email. The computing lead, with the support of the safeguarding manager, will have responsibility in checking that the account is being used appropriately.

All parents will be informed of the twitter account and be given the opportunity to withdraw from their child's photo or work being published on the account. Any withdrawals will be documented and shared with all members of staff. Parents will be encouraged to follow the school Twitter account but will be asked that it is not used as a way of contacting the school with queries. Parents will also be reminded that it is not appropriate to attempt to find and follow/friend members of staff on social media. Staff are asked not to reply to any query tweets and not follow or associate their personal twitter account to the school twitter account.

Care must be taken to ensure any tweets to other twitter accounts must reflect well on the school, be professional and be with the vision of sharing and promoting educational experiences. This may be tweeting accounts of visitors into school, authors, book publishers, charities and school trip locations.
Any inappropriate comments left on the twitter account should immediately be removed and reported to the headteacher.

Safeguarding Actions – Staff

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

In case of child pornography being found, the member of staff should be immediately suspending and the police should be called: anyone may report any inappropriate or potentially illegal activity or abuse towards a child online to the Child Exploitation and Online Protection (CEOP).

All staff will be asked to sign to say that they have read and understood the E-safety policy.

Teaching of E-Safety

Our E-Safety curriculum ensures that we are teaching the "knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device platform or app," (Teaching Online Safety in School, DFE, June 2019). We aim to teach our pupils to have a positive, yet sensible attitude towards the online world by ensuring that they have the "knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way," (Teaching Online Safety in School, DFE, June 2019). We also place a large emphasis on children understanding how they must behave online, not just the behaviour of others.

Meeting the needs of pupils

We also ensure that we tailor out teaching to "support to the specific needs of their pupils," (Teaching Online Safety in School, DFE, June 2019). This links to our Safeguarding Policy, Keeping Children Safe in Education and staff using their knowledge of pupils' background, experiences, ability, culture, language and any safeguarding concerns (including knowing which pupils are more likely to be susceptible to online harm e.g. SEND) when planning and adjusting lessons. Although the objectives below and planned out in to progressive key stage objectives, it is recognised that for some of our pupils it may be appropriate to re-visit objectives from previous key stages. Our I-Vengers (first implemented 2020/2021) are also used to support pupils' from a pupil's perspective. In addition to this, our learning mentor and/or outside agencies (such as Safe 'n' Sound) work with identified pupils to target specific needs.

Making our pupils feel safe

During lessons, children are in a safe environment where they are encouraged to show our FIRSY value of 'Respectful.' Children are encouraged to discuss ideas with each other. If children are feeling worried or wish to share anything with a member of staff, the whole school approach applies: put it in the classroom worry box; speak to the class teacher; or speak to a member of the safeguarding team.

Additional Opportunities

As well as teaching our E-Safety curriculum, every year our school takes part in Safer Internet Day and Anti-Bullying week: each class completes a range of activities that are suitable for their age group. We may also have visitors attend school to complete age and ability appropriate workshops such as Konflux Education. https://www.konfluxtheatre.co.uk/topics/internet-safety

In line with our Safeguarding policy we also have external visits from Safe 'n' Sound and the NSPCC, which may also cover aspects of online safety. https://www.nspcc.org.uk/keeping-children-safe/our-services/working-with-schools/
https://www.safeandsoundgroup.org.uk/

Our Curriculum

E-Safety at Firs is primarily taught discreetly for 1 half term every year, with revisiting as required by the needs of the pupils or as issues arise. Our E-Safety curriculum has been designed in line with guidance and other whole school curriculums: National Curriculum; PSHE (SCARF) curriculum; Derby Diocese Academy Curriculum Progression; Teaching Online Safety in School (DFE); and Education for a Connected World (UK Council for Internet Safety).

The curriculum has been designed to cover these strands of E-Safety identified from Teaching Online Safety in School and Education for a Connected World (UK Council for Internet Safety):

- Online Relationships
- Self Identity
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, well-being and lifestyle
- Copyright and ownership

The curriculum below is separated into key stages (KS1, LKS2, UKS2) and then split in to two progressive sections. These sections may be used when planning progression through lessons or through differentiation when planning lessons and determining outcomes for children. The objectives have been taken from the published document, Education for a Connected World (UK Council for Internet Safety).

The success criteria below does not determine how many lessons are required to cover each criteria: multiple criteria may be addressed within one lesson, or one statement may take multiple lessons to teach successfully. Each strand has been planned in to the two-year curriculum cycle at Firs. Every strand will not be covered every year, but every child who goes through their education at Firs will receive teaching in all of the strands by the end of Year 6. However, at any point in the school year, if a class teacher identifies the need for a particular strand to be addressed for individuals or their class, this may be planned in as an additional teaching opportunity.

National Curriculum

KS1 Objective: 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 Objective: use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

	EYFS (4+)	Key Stage 1		Lower Key Stage 2		Upper Key Stage 2	
Self-Identity	• I can recognise, online or offline, that anyone can say no/please stop/ I'll tell/ I'll ask to somebody who makes them feel sad, uncomfortable, embarrassed or upset	• I can recognise that there may be people online who could make someone feel sad, embarrassed or upset • If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust and how they can help.	• I can explain how other people may look and act differently online and offline • I can give examples of issues online that might make someone feel sad, worried, uncomfortable or frightened; I can give examples of how they might get help.	• I can explain what is meant by the term identity • I can explain how people can represent themselves in different ways online • I can explain ways in which someone might change their identify depending on what they are doing online (e.g. gaming; using an avatar; social media) and why	• I can explain how my online identity can be different to by offline identity • I can describe positive ways for someone to interact with others online and understand how this will positively impact on how others perceive them • I can explain that others online can pretend to be someone else including by friends, and can suggest reasons why they might do this	• I can explain how identity online can be copied, modified or altered. • I can demonstrate how to make responsible choices about having an online identity, depending on context.	• I can identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online. • I can describe issues online that could make anyone feel sad, worried, uncomfortable or frightened. I know and can give examples of how to get help, both on and offline. • I can explain the importance of asking until I get the help needed.
Online Reputation	• I can identify ways that I can put information on the internet	• I can recognise that information can stay online and could be copied • I can describe what information I should not put online without asking a trusted adult first	• I can explain how information put online about someone can last for a long time • I can describe how anyone's online information could be seen by others • I know who to talk to if something has been put online without consent or if it is incorrect.	• I can explain how to search for information about others online • I can give examples of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal • I can explain who someone can ask if they are unsure about putting something online	• I can describe how to find out information about others by searching online • I can explain ways that some of the information about anyone online could have been created copied or shared by others	• I can search for information about an individual online and summarise the information found • I can describe ways that information about anyone online can be used by others to make judgements about an individual, and why these may be incorrect.	• I can explain the ways in which anyone can develop a positive online reputation • I can explain strategies anyone can use to protect their 'digital personality' and online reputation, including degrees of anonymity.
	Additional guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf Schools can help pupils to identify and manage risk by: • discussing the ways in which someone may put themselves at risk online, • discussing risks posed by another person's online behaviour, • discussing when risk taking can be positive and negative, • discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example, discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with • • asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?						

Online Relationships	• I can recognise some ways in which they internet can be used to communicate • I can give examples of how I (might) use technology to communicate with people I know.	• I can give examples of when I should ask permission to do something online and explain why this is important • I can use the internet with adult support to communicate with people I know (e.g. video call apps or services). • I can explain why it is important to be considerate and kind to people online and to respect their choices. • I can explain why things one persons finds funny or sad online may not always be seen in the same way by others.	• I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. • I can explain who I should ask before sharing things about myself or others online. • I can describe different ways to ask for, give or deny my permission online and can identify who to ask for help if I am unsure. • I can explain why I have a right to say 'no' or 'I will have to ask someone.' I can explain who can help me if I feel under pressure to agree to something I am unsure about or don't want to do. • I can identify who can help me if something happens online without my consent. • I can explain how it may make others feel if I do not ask their permission or ignore their answers before sharing something about them online. • I can explain why I should always ask a trusted adult before clicking 'yes' 'agree' or 'accept' online	• I can describe ways people have similar likes and interests can get together online. • I can explain what it means to 'know someone' online and why this might be different from knowing someone offline. • I can explain what is meant by 'trusting someone online,' and why it is important to be careful about who to trust online including what information and content they are trusted with. • I can explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried. • I can explain how someone's feelings can be hurt by what is said or written online. • I can explain the importance of giving and gaining permission before sharing things online; how the principles of sharing online is the same as sharing offline .g. sharing images and videos.	• I can describe strategies for safe and fun experiences in a range of online social environments (e.g. live streaming, gaming platforms) • I can give examples of how to be respectful to others online and describe how to recognise healthy and unhealthy online behaviours. • I can explain how content shared online may feel unimportant to other people's thoughts, feelings and beliefs.	• I can give examples of technology specific forms of communication (e.g. emojis, memes and GIFS) • I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault. • I can describe some of the ways people may be involved in online communities and describe how they might collaborate constructively with others and make positive contributions (e.g. gaming communities or social media groups)	• I can explain how sharing something online may have an impact either positively or negatively. • I can describe how to be kind and show respect for others online including the importance of respecting boundaries regarding what is shared about them online and how to support them if others do not. • I can describe how things shared privately online can have unintended consequences for others (e.g. screen grabs).
	Additional guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf Schools can help pupils to recognise acceptable and unacceptable behaviour by: • looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do, • looking at how online emotions can be intensified resulting in mob mentality, • teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online, • considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.						

Online Bullying	• I can describe the ways that some people can be unkind online • I can offer examples of how this can make others feel	• I can describe how to behave online in ways that do not upset others and can give examples	• I can explain what bullying is, how people may bully others and how bullying can make someone feel. • I can explain why anyone who experiences bullying not to blame. • I can talk about how anyone experiencing bullying can get help.	• I can describe appropriate ways to behave towards other people online and why this is important. • I can give examples of how bullying behaviour could appear online and how someone can get support.	• I can recognise when someone is upset, hurt or angry online. • I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat) • I can explain why people need to think carefully about how content they post might affect others, their feelings and how it may affect how others feel about them (their reputation).	• I can recognise online bullying can be different to bullying in the physical world and can describe some of those differences. • I can describe how what one person perceives as playful joking and teasing (including 'banter') might be experienced by others as bullying. • I can explain how anyone can get help if they are being bullied online and identify when to tell a trusted adult. • I can identify a range of ways to report concerns and access support both in school and at home about online bullying. • I can explain how to block abusive users. • I can describe the helpline services which can help people experiencing bullying, and how to access them (e.g. Childline or The Mix).	• I can describe how to capture bullying content as evidence (e.g. screen grab, URL, profile) to share with others who can help me. • I can explain how someone would report online bullying in different contexts.
	Additional Guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf Schools can help pupils by: • helping them to identify who trusted adults are, • looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education) • helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.						

Managing Online Information	• I can talk about how to use the internet as a way of finding information online. • I can identify devices I could use to access information on the internet.	• I can give simple examples of how to find information using digital technologies, e.g. search engines, voice activated searching). • I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke. • I know how to get help from a trusted adult if we see content that makes us feel sad, uncomfortable worried or frightened.	• I can use simple keywords in search engines. • I can demonstrate how to navigate a simple webpage to get to information I need (e.g. home, forward, back buttons; links, tabs and sections). • I can explain what voice activated searching is and how it might be used, and know it is not a real person (e.g. Alexa, Google Now, Siri). • I can explain the difference between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'. • I can explain why some information I find online may not be real or true.	• I can demonstrate how to use key phrases in search engines to gather accurate information online. • I can explain what autocomplete is and how to choose the best suggestion. • I can explain how the internet can be used to sell and buy things. • I can explain the difference between a 'belief', an 'opinion' and a 'fact. and can give examples of how and where they might be shared online, e.g. in videos, memes, posts, news stories etc. • I can explain that not all opinions shared may be accepted as true or fair by others (e.g. monsters under the bed). • I can describe and demonstrate how we can get help from a trusted adult if we see content that makes us feel sad, uncomfortable worried or frightened.	• I can analyse information to make a judgement about probable accuracy and I understand why it is important to make my own decisions regarding content and that my decisions are respected by others. • I can describe how to search for information within a wide group of technologies and make a judgement about the probable accuracy (e.g. social media, image sites, video sites). • I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in-app purchases, pop-ups) and can recognise some of these when they appear online. • I can explain why lots of people sharing the same opinions or beliefs online do not make those opinions or beliefs true. • I can explain that technology can be designed to act like or impersonate living things (e.g. bots) and describe what the benefits and the risks might be. • I can explain what is meant by fake news e.g. why some people will create stories or alter photographs and put them online to pretend something is true when it isn't.	• I can explain the benefits and limitations of using different types of search technologies e.g. voice-activation search engine. I can explain how some technology can limit the information I aim presented with e.g. voice-activated searching giving one result. • I can explain what is meant by 'being sceptical'; I can give examples of when and why it is important to be 'sceptical'. • I can evaluate digital content and can explain how to make choices about what is trustworthy e.g. differentiating between adverts and search results. • I can explain key concepts including: information, reviews, fact, opinion, belief, validity, reliability and evidence. • I can identify ways the internet can draw us to information for different agendas, e.g. website notifications, pop-ups, targeted ads. • I can describe ways of identifying when online content has been commercially sponsored or boosted, (e.g. by commercial companies or by vloggers, content creators, influencers). • I can explain what is meant by the term 'stereotype', how 'stereotypes' are amplified and reinforced online, and why accepting 'stereotypes' may influence how people think about others. • I can describe how fake news may affect someone's emotions and behaviour, and explain why this may be harmful. • I can explain what is meant by a 'hoax'. I can explain why someone	• I can explain how search engines work and how results are selected and ranked. • I can explain how to use search technologies effectively. • I can describe how some online information can be opinion and can offer examples. • I can explain how and why some people may present 'opinions' as 'facts'; why the popularity of an opinion or the personalities of those promoting it does not necessarily make it true, fair or perhaps even legal. • I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how someone might encounter these online (e.g. advertising and 'ad targeting' and targeting for fake news). • I understand the concept of persuasive design and how it can be used to influences peoples' choices. • I can demonstrate how to analyse and evaluate the validity of 'facts' and information and I can explain why using these strategies are important. • I can explain how companies and news providers target people with

						would need to think carefully before they share.	online news stories they are more likely to engage with and how to recognise this. • I can describe the difference between online misinformation and dis-information. • I can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen (e.g. the sharing of misinformation or disinformation). • I can identify, flag and report inappropriate content
Health, well-being and lifestyle	• I can identify rules that help keep us safe and healthy in and beyond the home when using technology. • I can give some simple examples of these rules.	• I can explain rules to keep myself safe when using technology both in and beyond the home.	• I can explain simple guidance for using technology in different environments and settings e.g. accessing online technologies in public places and the home environment. • I can say how those rules / guides can help anyone accessing online technologies.	• I can explain why spending too much time using technology can sometimes have a negative impact on anyone, e.g. mood, sleep, body, relationships; I can give some examples of both positive and negative activities where it is easy to spend a lot of time engaged (e.g. doing homework, games, films, videos). • I can explain why some online activities have age restrictions, why it is important to follow them and know who I can talk to if others pressure me to watch or do something online that makes me feel uncomfortable (e.g. age restricted gaming or web sites).	• I can explain how using technology can be a distraction from other things, in both a positive and negative way. • I can identify times or situations when someone may need to limit the amount of time they use technology e.g. I can suggest strategies to help with limiting this time.	• I can describe ways technology can affect health and well-being both positively (e.g. mindfulness apps) and negatively. • I can describe some strategies, tips or advice to promote health and wellbeing with regards to technology. • I recognise the benefits and risks of accessing information about health and well-being online and how we should balance this with talking to trusted adults and professionals. • I can explain how and why some apps and games may request or take payment for additional content (e.g. in-app purchases, lootboxes) and explain the importance of seeking permission from a trusted adult before purchasing.	• I can describe common systems that regulate age-related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose. • I recognise and can discuss the pressures that technology can place on someone and how / when they could manage this. • I can recognise features of persuasive design and how they are used to keep users engaged (current and future use). • I can assess and action different strategies to limit the impact of technology on health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and exercise).

	Additional Guidance https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf Schools can help pupils to recognise: • 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, • ways in which games and social media companies try to keep users online longer (persuasive/sticky design) • criminal activities such as grooming.						
Privacy and Security	• I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location). • I can describe who would be trustworthy to share this information with; I can explain why they are trusted.	• I can explain that passwords are used to protect information, accounts and devices. • I can recognise more detailed examples of information that is personal to someone (e.g where someone lives and goes to school, family names). • I can explain why it is important to always ask a trusted adult before sharing any personal information online, belonging to myself or others.	• I can explain how passwords can be used to protect information, accounts and devices. • I can explain and give examples of what is meant by 'private' and 'keeping things private' • I can describe and explain some rules for keeping personal information private (e.g. creating and protecting passwords). • I can explain how some people may have devices in their homes connected to the internet and give examples (e.g. lights, fridges, toys, televisions).	• I can describe simple strategies for creating and keeping passwords private. • I can give reasons why someone should only share information with people they choose to and can trust. I can explain that if they are not sure or feel pressured then they should tell a trusted adult. • I can describe how connected devices can collect and share anyone's information with others.	• I can describe strategies for keeping personal information private, depending on context. • I can explain that internet use is never fully private and is monitored, e.g. adult supervision. • I can describe how some online services may seek consent to store information about me; I know how to respond appropriately and who I can ask if I am not sure. • I know what the digital age of consent is and the impact this has on online services asking for consent.	• I can explain what a strong password is and demonstrate how to create one. • I can explain how many free apps or services may read and share private information (e.g. friends, contacts, likes, images, videos, voice, messages, geolocation) with others. • I can explain what app permissions are and can give some examples.	• I can describe effective ways people can manage passwords (e.g. storing them securely or saving them in the browser). • I can explain what to do if a password is shared, lost or stolen. • I can describe how and why people should keep their software and apps up to date, e.g. auto updates. • I can describe simple ways to increase privacy on apps and services that provide privacy settings. • I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. scams, phishing). • I know that online services have terms and conditions that govern their use.

Copyright and Ownership	• I know that work I create belongs to me. • I can name my work so that others know it belongs to me.	• I can explain why work I create using technology belongs to me. • I can say why it belongs to me (e.g. 'I designed it' or 'I filmed it''). • I can save my work under a suitable title / name so that others know it belongs to me (e.g. filename, name on content). • I understand that work created by others does not belong to me even if I save a copy	• I can recognise that content on the internet may belong to other people • I can describe why other people's work belongs to them.	• I can explain why copying someone else's work from the internet without permission isn't fair and can explain what problems this might cause.	• When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it. • I can give some simple examples of content which I must not use without permission from the owner, e.g. videos, music, images.	• I can assess and justify when it is acceptable to use the work of others. • I can give examples of content that is permitted to be reused and know how this content can be found online.	• I can demonstrate the use of search tools to find and access online content which can be reused by others. • I can demonstrate how to make references to and acknowledge sources I have used from the internet.
	Key Questions: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf • is this website/URL/email fake? How can I tell? • what does this cookie do and what information am I sharing? • is this person who they say they are? • why does someone want me to see this? • why does someone want me to send this? • why would someone want me to believe this? • why does this person want my personal information? • what's behind this post? • is this too good to be true? • is this fact or opinion?						

Remote Learning Addendum to the E-Safety Policy

We have devised some guidance that reflects the changed circumstances brought about by Covid-19 and the significant increase in the use of online technology to facilitate teaching and learning. This addendum does not introduce any new concepts, rather, it specifically outlines the various applications used for the delivery of online classes remotely.

This guidance operates alongside all of our existing policies which can be viewed on our school website. We continue to expect all staff to abide by the highest professional standards when working directly and remotely with students and our Safeguarding Policy and Staff Code of Conduct still currently apply. Students must comply with this additional guidance and we request that parents/carers ensure that their child fully understands and agrees to follow these guidelines.

Introduction

This document sets out the guidance in respect to the use of technology to facilitate remote teaching and learning, hereafter referred to as "Remote Learning." This addendum will be kept under review as circumstances dictate.

Scope of this Guidance

This guidance covers any aspect of student remote learning as used by staff.

The list of applications that will be used for remote learning will primarily be:

- MyOn
- Zoom
- ClassDojo
- MyMaths
- School Website
- YouTube

Remote Learning Approach

Remote Learning will incorporate a number of different approaches including the use of live classes either filmed or audio only and or shared workspaces. All teachers will aim to provide the best experience for students that provides feedback and interaction but will adopt different approaches (live teaching, pre-recorded lessons etc.). In all cases our primary aim is to cover the required curriculum for all subject areas. Students should get in touch with their teacher right away if they are having difficulty with any aspect of their learning or contact the school office if they are struggling to access the remote learning.

Responsibilities while engaging in Remote Learning

For staff:

- Teachers have overall control of the online interaction of their class.

- Any student that disrupts the lesson and does not respond positively to the teacher's instructions will be removed in order to allow those who wish to partake a fair chance to do so. A student who repeatedly disrupts learning may receive a temporary ban from all online access.
- In the event of a bubble closure, teachers will do their utmost to be available during school learning hours – this may be via a zoom video or through class dojo.
- In the event of single student isolation, teachers will do their utmost to provide feedback to pupils and answer any questions either before or after school.
- Staff will remind students of the expectations in terms of behaviour during live sessions and the conduct expected of them.
- Where possible, there will be two members of staff online during live teaching sessions, or the session will be recorded and stored following the session.

For students:

- You must always be polite and respectful to your teachers and fellow students.
- You are not to film (by any means) or forward any content within the lesson
- You understand that all your online activity is monitored. This includes anything on Dojo and the learning platform, and whether you are checking regularly for assigned work.

For parents/carers:

- You should ensure that your child is checking in regularly for assigned work.
- When your child is watching a live lesson, you should try to ensure your child is in an area of the house that is quiet and free from distractions.
- We would insist that students do not try to film the session using any device.
- A live online lesson must be treated like a regular school lesson and only viewed by those who are invited to attend.

This guidance is in line with the Positive Behaviour Policy Addendum

https://firsprimary.derby.sch.uk/wp-content/uploads/2020/09/Positive-Behaviour-Policy-COVID-19-Sept-2020.pdf

Live Online Classes

Teachers may deliver some of the lesson "live" using Zoom. This will use varying combinations of audio, video, virtual whiteboards and screencasts.

In the use of Zoom:

- Students must always follow the direction of their teacher just as in the classroom.
- Students are not to film the session using any device.
- Students are not to turn on their microphone unless the teacher invites them to do so. All microphones should be on mute when a person is not speaking to avoid distracting background noise being broadcast to everyone.
- A live lesson is intended for the allocated class only. The teacher will decide who should receive the invite through ClassDojo. Only those invited by the teacher have permission to view the lesson.
- Staff may pre-record a lesson prior to sharing it with pupils, or record a live lesson.

References

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19#virtual-lessons-and-live-streaming

Online safety

During the current situation, student screen time will inevitably be increased significantly, both for home learning and personal use. The school is committed to keeping children safe online and to ensuring positive online interaction between teachers, parents and pupils. Some work should also be set which is not computer-based, to allow pupils learning time away from screens.

Pupils will be given guidance in line with the DfE guidance on 'Teaching about online safety', June 2019. Pupils will be taught:

- Appropriate online behaviour
- How to evaluate what they see online
- How to identify online risks
- How to recognise techniques used for persuasion
- How and when to seek support

Parents should be aware of:

- The importance of remaining in control of electronic devices at home and remaining in earshot when children are in contact with teachers.
- What their children are being asked to do online during this period of remote learning.
- The sites that the children will be asked to access.
- Filters that might be appropriate on home computers if online lessons are to be effective.
- Who their child is going to be interacting with online.
- How to report concerns to the school.
- Where to seek support to help them to keep their children safe online.
- The following websites offer support to parents and carers regarding e-safety:
    - Internet matters https://www.internetmatters.org
    - London Grid for Learning https://www.lgfl.net/default.aspx
    - Net-aware https://www.net-aware.org.uk
    - Thinkuknow https://www.thinkuknow.co.uk/
    - Parent Info https://parentinfo.org/
    - UK Safer Internet Centre https://www.saferinternet.org.uk

Staff should:

- Reinforce e-safety messages during lessons and when setting homework that requires access to the Internet.
- Encourage students to be critically aware of the content they access on-line and be guided to validate the accuracy of information, acknowledge the source of information used, avoid plagiarism and respect copyright.
- Be alert to possible peer-on-peer abuse. This could occur during online collaborative work on a Zoom session. Teachers must control these sessions and report concerns. No additional unsupervised online collaborative work should be encouraged.
- Check what is visible on screen to the pupil, so that nothing inappropriately personal is visible (e.g. personal item, painting, poster)
- Make sure that there is never a possibility of strangers having access to the screen.
- Check thoroughly any pictures or video-clips that we want to share with pupils

- Report immediately any concerns about online safety of pupils to the DSL or one of the deputies. Any such concerns should be dealt with as per our Safeguarding policy and where appropriate referrals should still be made to children's social care and as required by the police.

Staff should be aware of the UK Safer Internet Centre's professional online safety helpline, which provides support with any online safety issues which they may face:

https://www.saferinternet.org.uk/helpline/professional

Staff can also signpost children to age appropriate practical support from:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse