St. Helen's College

Online Safety Policy

This is a whole-school policy which includes the Early Years Foundation Stage.

Designated Safeguarding Lead (DSL) team	**DSL: Mrs Melanie Gilbert** **mgilbert@sthelenscollege.com 01895 234371** **Deputy DSL and Head of Pre-Prep: Ms Jo Matthews** **jmatthews@sthelenscollege.com 01895 272967**
Link governor for safeguarding (includes online safety)	**Chairman** **Mr. John Forsyth** **jf@forfareducation.co.uk** **07443 103805** **Basia Lubaczewska** **Safeguarding Governor** **safeguarding@forfareducation.co.uk**
Deputy Head Academic	**Mr Steve Roche** **sroche@sthelenscollege.com**
Head of Computing	**Mrs. Ashley Coker** **acoker@sthelenscollege.com**
PSHE/RSHE/RSE lead	**Mrs. Poonam McLaughlin** **pmclaughlin@sthelenscollege.com**
Network manager	**Mr. Pal Puchinszki** **ppuchinszki@sthelenscollege.com**

Online safety educational content focuses on four key areas, as highlighted in Keeping Children Safe in Education (KCSiE) September 2025:

Content: Being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;

Contact: Being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults;

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm; e.g. making, sending and receiving explicit images, or online bullying; and

Commerce: risks such as online gambling, inappropriate advertising, phishing and /or financial scams.

1. Introduction

This policy provides guidance on the responsible use of the internet and seeks to ensure the safety of pupils.

The effective use of the variety of applications made possible by the internet is an essential life skill that should be developed in children by the school and at home. Whilst providing access to the internet, the school must guard against the possibility of pupils being placed in embarrassing, inappropriate or dangerous situations.

We believe the best approach is by fostering a responsible attitude in our pupils in partnership with parents. This is supported in school by a combination of site-filtering and adult supervision.

This policy should be referred to alongside the following guidance:
- The Independent School Standards Regulations (ISSRs)
- The Statutory framework for the EYFS
- Education and Skills Act 2008
- Children Act 1989
- Childcare Act 2006
- The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
- The Equality Act 2010
- Keeping Children Safe in Education (KCSiE) 2025
- DfE Behaviour Guidance 2024
- Teaching online safety in schools (DfE, 2023)
- Harmful online challenges and online hoaxes (DfE, February 2021)
- Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (DfDCMS 2020)
- UK Council for Internet Safety (UKCIS) - Education for a Connected World, 2020.

2 Using the internet in teaching and learning

The internet provides access to vast amounts of information, allows self-directed, independent learning through interactive applications and provides a collaborative working environment. Staff and pupils use information and online applications as part of their school day. Pupils are expected to use online resources at home to complete homework tasks and communicate with teachers about their work using the online school learning platform.

The children will be taught about the benefits and risks of using the internet and they will learn how to use it safely and effectively. Key objectives taught for each year group can be seen in Appendix 1. They will be taught about appropriate use of email and social media sites. This will be reinforced in our year-round online safety curriculum and an annual online safety day. This is supplemented by further sessions in our Computing and PSHCE and RSE curriculums. Parents will be invited to attend annual training regarding online safety. The school also sends frequent, topical information on online safety issues to parents.

The school will educate pupils about the vast resources available on the internet. Initially the pupils may be restricted to sites which have been reviewed and selected for content. As pupils gain experience, they will be taught how to use searching techniques to locate specific information independently. Pupils will be taught to be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.

All staff will review and evaluate the educational resources available as apps and on web sites. The Computing Subject Leader will assist in the evaluation of these resources.

At St. Helen's College, we recognise that online safety and broader digital resilience must be woven throughout the curriculum and that is why we have adopted the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety). We achieve this through a combination of sessions in our Computing, PSHCE and RSE curriculums.

3.Appropriate use and managing internet access

As with other forms of media such as books, magazines and videos, some content available on the internet may be unsuitable for pupils. The School takes all reasonable steps to ensure that users can

access only appropriate material. This is managed through the School's web-filtering system, LGfL SchoolProtect, which helps safeguard pupils while they are online.

Children will only be allowed to use the internet in public areas of the school, such as the library or in the classroom, when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen and the school cannot accept liability for the material accessed, or any consequences of internet access. Strong filtering systems and active monitoring work to mitigate potential risks.

If staff or pupils encounter inappropriate or unsuitable online content, the screen should be turned off immediately to prevent any further exposure. The website address and details of the content must be reported promptly to the Network Manager and the Designated Safeguarding Lead (DSL), and appropriate steps will be taken to block further access.

Any content that the school believes may be illegal will be reported to the Internet Watch Foundation. The school will regularly review its procedures and control measures to identify, assess, and minimise online safety risks.

Members of staff will be aware of the potential for misuse and will be responsible for explaining to pupils the expectation we have of them.

Cyber-bullying will be treated in line with the School's Anti-Bullying Policy. Inappropriate emails or postings to social networking sites, whether made from home or the school, will result in disciplinary action, which may include temporary or in extreme cases permanent exclusion from school. If excluded from school, the student's school accounts may be suspended.

4 Authorising internet access

Access to the internet will be under the direction of an adult.

Parents will be informed that pupils will be provided with directed internet access and they will be asked to sign and return a consent form as part of the acceptance paperwork before their child joins the school. At the start of each academic year, children in Year 2 and above sign an agreement published in their homework diaries; this can be seen in Appendix 3.

Rules for internet access are posted in the computer lab and school information boards. Pupils are informed that internet use will be monitored.

Instruction in responsible and safe use precede internet access being given and responsible internet use is reinforced regularly.

5 Management of online safety concerns / incidents

It is vital that all staff recognise that online safety is a part of safeguarding.

General concerns must be handled in the same way as any other safeguarding concern and be reported to a designated safeguarding lead.

School procedures for dealing with online safety issues are detailed in the following policies :

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Digital and Technology Acceptable Use Policy
- Low Level Concerns Policy
- Prevent Risk Assessment
- Relationship and Sex Education Policy
- Social Media Policy

The school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur inside and outside of school, where access is out of our control. All members of the

school community are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Appendices:

Appendix 1 - Year group objectives taught
Appendix 2 - Responsible internet use agreements (signed by parents upon joining the school)
Appendix 3 - Responsible internet use code of conduct (in each child's reading record)
Appendix 4 - Useful websites
Appendix 5 - Roles and Responsibilities

Appendix 1

Year group objectives

Early Years Foundation Stage (EYFS)

- I can name and recognise uncomfortable, embarrassed and upset emotions.
- I can recognise, online or offline, that anyone can say 'no thank you'/'please stop' / 'I'll tell' / 'I'll ask' to somebody who makes them feel sad, uncomfortable, embarrassed or upset.
- I can recognise some ways in which the internet can be used to communicate.
- I can give examples of how I (might) use technology to communicate with people I know.

  I can identify ways that I can put information on the internet.
- I can describe ways that some people can be unkind online.
- I can offer examples of how this can make others feel.
- 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 identify rules that help keep us safe and healthy in and beyond the home when I am using technology.
- I can give simple examples of these rules.
- I can apply these rules during my play.
- I can link feelings to my online experiences.
- I can identify some simple examples of personal information (eg. 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 know that work I create belongs to me.
- I can name my work so that others know it belongs to me.
- I can express how I felt when I created this work.
- I can share my work with a friend.

Year 1

- 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 give examples of when I should ask permission to do something online and explain why this is important.
- I can recognise some ways in which the internet can be used to communicate.
- I can give examples of how I (might) use technology to communicate with people I know

- 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 person finds funny or sad online may not always be seen in the same way by others.
- I can identify ways that I can put information on the internet.

- I can describe what information I should not put online without asking a trusted adult first.
- 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 describe ways that some people can be unkind online.
- I can offer examples of how being unkind can make others feel.
- I can describe how to behave online in ways that do not upset others and can give examples.
- 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 (eg. search engines, voice-activated searching).
- I understand that I can encounter a range of things online, including things I 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 I see content that makes me feel sad, uncomfortable, worried or frightened.
- I can give some simple examples of the rules to keep me safe online.
- I can explain rules to keep myself safe when using technology both in and beyond the home.
- I can explain rules to keep myself safe when using technology both in and beyond the home.
- I can identify some simple examples of my personal information (eg. name, address, birthday, age, location).
- I can explain why it is important to always ask a trusted adult before sharing online and personal information belonging to myself or others.
- I can recognise more detailed examples of information that is personal to someone (eg. where someone lives and goes to school, family names).
- 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 know that the work I create belongs to me.
- I can name my work so that others know it belongs to me.
- I can explain why the work I create using technology belongs to me.
- I can say why it belongs to me (eg. 'I designed it' or 'I filmed it').
- I understand that work created by others does not belong to me even if I save a copy.

Year 2

- 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 describe some risks online and what I can do to stay safe.
- 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 (eg. email, online gaming, a pen-pal in another school/country).
- 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 can help me if I am not sure.
- I can explain why I should always ask a trusted adult before clicking 'yes', 'agree' or 'accept' online.
- I can explain why I have the 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 how information put online about someone can last for a long time.

- I can describe how anyone's 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 what bullying is, how people may bully others and how bullying can make someone feel.
- I can explain why anyone who experiences bullying is not to blame.
- I can talk about how anyone experiencing bullying can get help.
- I can use simple keywords in search engines.
- I can demonstrate how to navigate a simple webpage to get the information I need (eg. home, forward, back buttons; links, tabs and sections).
- I can explain what voice activated searching is and how it might be used, and I know it is not a real person (eg. 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 explain simple guidance for using technology in different environments and settings (eg. accessing online technologies in public places and the home environment).
- I can say how rules / guides can help anyone accessing online technologies.
- I can say how rules / guides can help anyone accessing online technologies.
- I can explain and give examples of what is meant by 'private' and 'keeping things private'.
- I can explain how passwords can be used to protect information, accounts and devices.
- I can describe and explain some rules for keeping personal information private (eg. creating and protecting passwords).
- I can explain how some people may have devices in their homes connected to the internet and give examples (eg. lights, fridges, toys, televisions).
- 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 describe why other people's work belongs to them.
- I can recognise that content on the internet may belong to other people.

Year 3

- 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 identity depending on what they are doing online (e.g. gaming, using an avatar, social media) and why.
- I can describe ways people who 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', why this is different from 'liking 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 are the same as sharing offline (e.g. sharing images and videos).
- 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 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 explain how to get support if someone is unkind online
- 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 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).
- 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 explain that not all opinions shared may be accepted as true or fair by others (e.g. monsters under the bed).
- I can explain why spending too much time using technology can sometimes have a negative impact (e.g. mood, sleep, body, relationships).
- I can give some examples of 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 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 unsure or feel pressured, they should tell a trusted adult.
- I can describe how connected devices can collect and share anyone's information with others.
- I can explain why copying someone else's work from the internet without permission isn't fair and what problems this might cause.
- I can save my digital work in different programs.

Year 4

- I can explain how my online identity can be different from my 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 my friends, and I can suggest reasons why they might do this.
- I can describe strategies for safe and fun experiences in a range of online social environments (e.g. livestreaming, 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 one person but may be important to other people's thoughts, feelings and beliefs.
- 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 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 describe ways people can be bullied through a range of media (e.g. image, video, text, chat).
- I can recognise when someone is upset, hurt or angry online.

- I can explain why people need to think carefully about how content they post might affect others and their feelings and how it may affect how others feel about them (their reputation).
- 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 some of the methods used to encourage people to buy things online (e.g. advertising offers, in-app purchases, pop-ups), and I can recognise some of these when they appear online.
- 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 explain what is meant by fake news, for example, 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 why lots of people sharing the same opinions or beliefs online does not make those opinions or beliefs true.
- 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 I can recognise some of these when they appear online.
- I can explain how using technology can be a distraction from other things in both a positive and negative way.
- I can identify times and situations when someone may need to limit the amount of time they use technology. I can suggest strategies to help with limiting this time.
- I can describe positive benefits to spending time away from technology
- I can describe strategies for keeping personal information private, depending on the context.
- I can explain that internet use is never fully private and is monitored.
- 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 give some simple examples of content which I must not use without permission from the owner (e.g. videos, music, images).
- 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.

Year 5

- 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 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 explain how someone can get help if they are having problems and identify when to tell a trusted adult.
- I can give examples of technology- specific forms of communication (e.g. emojis, memes and GIFs).
- 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 demonstrate how to support others (including those who are having difficulties) online.
- I can explain that information about other people online might not be correct and build a positive profile of myself online.
- 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 judgments about an individual and why these may be incorrect.

- I can recognise that online bullying can be different to bullying in the offline 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 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 who are experiencing bullying and how to access them (e.g. Childline or The Mix).
- I can explain the benefits and limitations of using different types of search technologies, for example voice- activation search engines. I can explain how some technology can limit the information I am presented with, for example 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, for example 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 would need to think carefully before they share.
- I can describe ways technology can affect health and well- being positively (e.g. mindfulness apps) and negatively.
- I can describe some strategies, tips or advice regarding technology to promote health and wellbeing.
- 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 well- being 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, loot boxes) and explain the importance of seeking permission from a trusted adult before purchasing.
- 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 give examples of content that is permitted to be reused and know how this content can be found online.
- I can assess, and justify when it is acceptable to use, the work of others.
- I can review rules about using other people's work online.

Year 6

- 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 can give examples of how to get help, both online and offline.
- I can explain the importance of asking until I get the help needed.
- I can talk about what I have learned in online safety lessons this year.
- 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, for example screengrabs.
- I can explain that taking or sharing inappropriate images of someone (e.g. embarrassing images), even if they say it is okay, may have an impact for the sharer and others; and I can
- explain who can help if someone is worried about this.
- I can give examples of when I should ask permission to do something online and explain why this is important.
- I can explain strategies anyone can use to protect their digital personality and online reputation, including degrees of anonymity.
- I can explain the ways in which anyone can develop a positive online reputation.
- I can show myself online in a positive way.
- 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.
- I can talk about the impact of online bullying and I know how to seek help
- 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 define the terms 'influence', 'manipulation' and 'persuasion' and explain how someone might encounter these online, for example advertising, ad targeting and targeting for fake news.
- I understand the concept of persuasive design and how it can be used to influence
- peoples' choices.
- I can demonstrate how to analyse and evaluate the validity of facts and information, and I can explain why using these strategies is important.
- I can explain how companies and news providers target people with online news stories they are more likely to engage with and how to recognise that
- I can describe the difference between online misinformation and disinformation.
- 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, for example the sharing of misinformation or disinformation.
- I can describe how some online information can be an opinion and can offer examples.
- I can explain how and why some people may present opinions as facts and 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 identify, flag and report inappropriate content.
- I can describe how some online information can be an opinion and can offer examples.
- I can explain how and why some people may present opinions as facts and 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 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).
- I can describe common systems that regulate age-related content (e.g. PEGI, BBFC,
- parental warnings) and describe their purpose.
- I can recognise features of persuasive design and how they are used to keep users engaged (current and future use).
- I recognise and can discuss the pressures that technology can place on someone and how/when they could manage this.
- I can describe effective ways people can manage passwords, for example 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, for example auto updates.
- 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 can describe simple ways to increase privacy on apps and services that provide privacy settings.
- I know that online services have terms and conditions that govern their use.
- I can spot phishing emails or scam messages when I am online and describe what to do if I am concerned about a message I have received.
- 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.
- I can reference someone else's piece of work or image that I have found online.

Appendix 2

Pupil Internet and Online Safety Rules

- I will ask permission before using the internet and will use only my own network login and password, which is secret.
- I will only use messaging systems supplied by the school and will only look at or delete my own files. I will not bring software or disks into school without permission.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and the internet sites I visit.
- I will at no time post messages about pupils or staff on any website.
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of messages and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Your signature below confirms that your child may access the internet in school as directed by staff. You will support the School in teaching your child online safety and ensuring that their access to systems/apps/software is age-appropriate. You understand that the School will take reasonable precautions to ensure pupils cannot access inappropriate material. You understand that the School cannot be held responsible for the nature or content of materials accessed through the internet. You agree that the school is not liable for damages arising from use of the internet.

Taking, Storing and Using Images of Children

The School uses pupil images to enhance pupils' educational experiences, to celebrate the achievements of pupils, to promote the work of the school, and for important administrative purposes such as identification and security. To comply with the General Data Protection Regulations, we must ask parents to opt-in to allow us to use pupil photographs. Photographs are always used in accordance with school policies, including our Safeguarding & Child Protection Policy, our Taking, Storing and Using Images of Children Policy and our Privacy Policy. These are available on the school website and we would encourage you to read them if you have any concerns or questions before signing this form.

Your signature below confirms that the School may use photographs/videos of your child for the purposes outlined above.

Signature:	
Print name:	
Relationship to child:	
Date:	

Appendix 3

St. Helen's College
Responsible Digital Citizenship

These rules help us to be fair to others and keep everyone safe.

- I will not use the internet without permission from an adult.
- I will use only my own login and password, which I will keep secret.
- I will not use my private email to communicate with teachers and will not use it at school.
- I will not use the internet to be unkind to others.
- I will not use internet chat at school and will only use messaging systems supplied by the school.
- I will not use any personal devices that can use public networks.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a member of staff immediately.
- I understand that the school may check my computer files, emails and the internet sites I visit.
- I will at no time post messages about pupils or staff on any public website or social media.
- I understand that I must not bring software, devices or data files into school without permission.
- I understand that if I deliberately break these rules, I may not be allowed to use the school systems or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web sites, the interception of messages and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix 4

Useful websites

Child Exploitation and Online Protection Centre (CEOPS) A UK policing agency dedicated to eradicating the sexual abuse of children.	www.ceop.police.uk
Bullying Online Advice for children, parents and schools	www.bullying.co.uk
Internet Watch Foundation - Invites users to report illegal Web sites	www.iwf.org.uk
Childnet	www.childnet.com
National Online Safety	https://nationalonlinesafety.com/
Education for a Connected World	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf
NSPCC	https://www.nspcc.org.uk/

Appendix 5

Roles and responsibilities

The Governing Body has overall responsibility for all matters which are the subject of this policy and is required to ensure that all those with leadership and management responsibilities at the School actively promote the online well-being of pupils.

Governors	● To ensure that the school follows all current online safety advice to keep the children and staff safe ● To approve the Online Safety Policy and review the effectiveness of the policy ● To support the school in encouraging parents and the wider community to become engaged in online safety activities ● To regularly review with the DSL ● To ensure that the School has appropriate filtering and monitoring systems in place and to regularly review their effectiveness, in order to demonstrate they are doing all they reasonably can to limit children's exposure to risks
Head and Designated Safeguarding Leads	● To take overall responsibility for online safety provision as part of safeguarding and child protection ● To manage safeguarding incidents involving use of technology in the same way as other safeguarding matters, in accordance with the Safeguarding Policy and procedures ● To liaise with the Network Manager to monitor technology use and practice across the school and assess whether any improvements should be made to ensure the online safety and wellbeing of pupils ● To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements ● To be responsible for ensuring that staff receive suitable training to carry out their online safety roles ● To review the Online Safety Policy ● To promote an awareness and commitment to online safeguarding throughout the school community ● To ensure that online safety education is embedded across the curriculum ● To facilitate training and advice for all staff
Head of Computing / Deputy Head Academic	● To oversee the delivery of the online safety element of the Computing curriculum
Network Manager	● To report any online safety related issues that arise, to the DSL ● To ensure that provision exists for virus and security threats (e.g. keeping virus protection up to date)

	● To keep up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant ● To regularly monitor the use of the school network in order that any misuse or attempted misuse can be reported to the DSL
All staff	● To read, understand and help promote the school's Online Safety Policy and guidance ● To read, understand and adhere to the Information Security and Acceptable Use Policy ● To report any suspected misuse or problem to the DSL ● To maintain an awareness of current online safety issues and guidance ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through school-based systems
Pupils	● To read, understand, sign and adhere to the Responsible Internet Use agreement (In Year 2 and above) ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they, or someone they know, feels worried or vulnerable when using online technology
Parents/carers	● To read, sign and understand the school's Responsible Internet Use agreement ● To support the school in promoting online safety at home