St Edward's Primary School
Online Safety Policy

The Governing Body of St Edward's CE Primary School adopted this policy on_____.

Signed _____ (Chair of Governors)

Introduction

St Edwards's Primary School recognises the internet and other digital technologies provide a good opportunity for children and young people to learn. These technologies allow all those involved in the education of children and young people to promote creativity, communicate with others, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at *St Edward's Primary School* want to ensure that technology is used to:

- Raise standards.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to learn in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

We are committed to an equitable learning experience for all pupils using technology and we recognise that technology can give pupils with SEND increased access to the curriculum to enhance their learning.

We are committed to ensuring that **all** pupils will be able to use technology safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

S*t Edward's Primary School* will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- teaching on e-safety integrated into the curriculum for all children
- a range of policies including safeguarding and acceptable use policies that are frequently reviewed and updated
- regular information to parents that highlights safe practice when using technology
- regular training for all staff on e-safety
  close supervision of pupils when using technology including robust internet filtering and a monitoring and reporting procedure for abuse and misuse

St Edward's Primary School expects all staff and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below: These expectations are also applicable to any staff and volunteers who work in school.

<u>Users are not allowed to:</u>

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children

- Promoting discrimination or extremism of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; racist or religious hatred material

The school recognises that in certain planned curricular activities, access to sites otherwise deemed inappropriate may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and extremism
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

Reporting Abuse

There may be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive or inappropriate material. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident immediately to SLT.

The school also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances safeguarding procedures should be followed. The response of the school will be to take the reporting of such incidents seriously and where judged necessary, the Designated Safeguarding Lead will refer details of an incident to Children's Social Care or the Police.

The school, as part of its safeguarding duty and responsibilities will assist and provide information and advice in support of child protection enquiries and criminal investigations.

Education and Training

St Edward's Primary School recognises that technology can transform learning; help to improve outcomes for children and young people and promote creativity.

We realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use technology safely.

To this end we will:
Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of technology. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

> **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
>
> **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
>
> **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;
>
> **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Training needs of all school staff will be regularly audited and training provided to improve their knowledge and expertise in the safe and appropriate use of technology.

Work closely with families to help them ensure that their children use technology safely and responsibly both at home and school. We will also provide them with relevant information on e-safety policies and procedures through our newsletters, Parent Forums and the school website and social media.

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead, IT technical support, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and filtering and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy

Designated Safeguarding Lead (DSL)
The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the governors to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Curriculum Leads
Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme.

- This will be provided through:
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they immediately report any suspected misuse or problem a DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Monitoring and Filtering

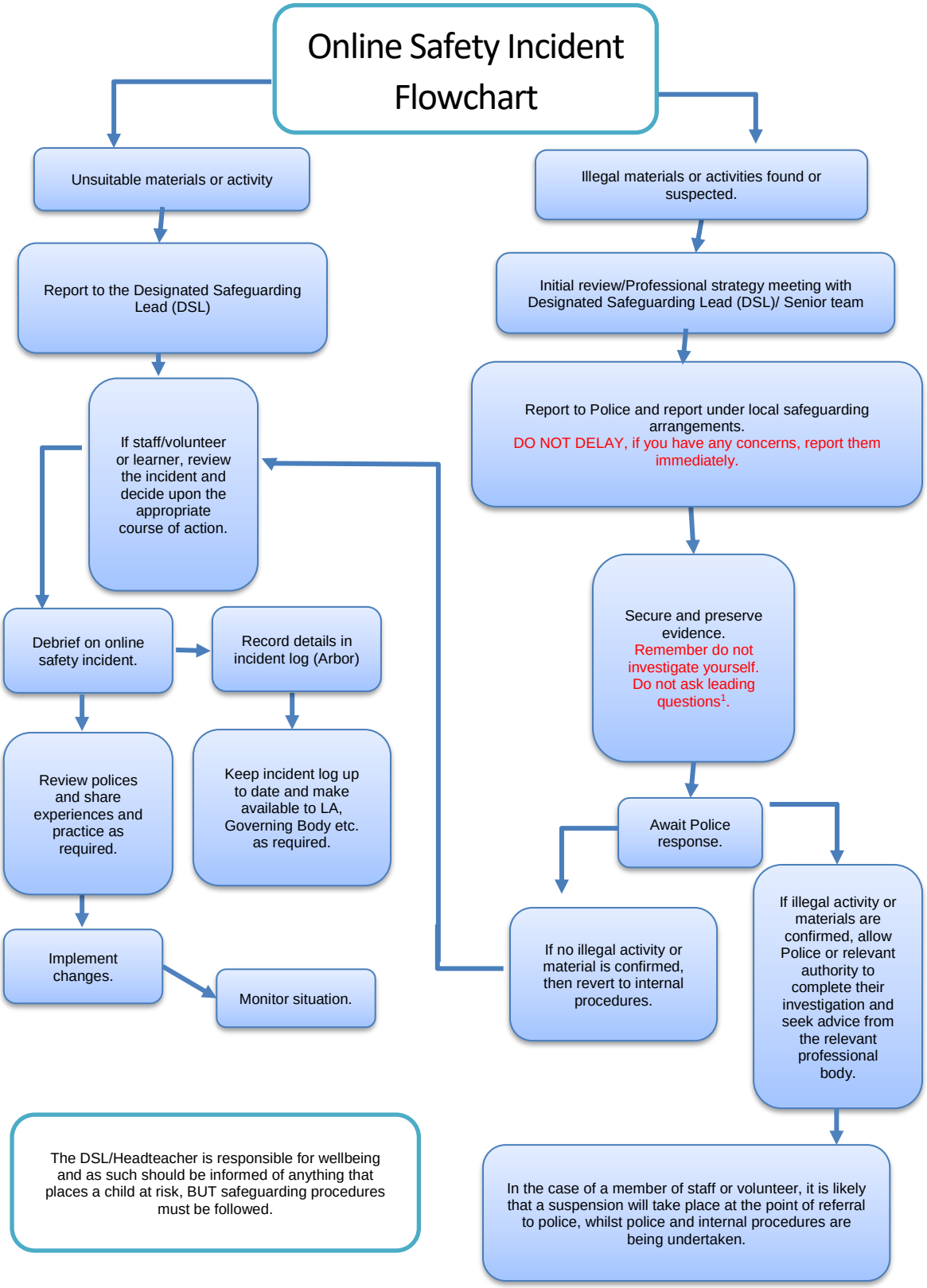
Monitoring the safe use of technology includes both the personal use of the internet and e-mail and the monitoring of patterns and trends of use.

Smoothwall Monitoring system filters and monitors use of devices within school used by students. The monitoring system is a live system sending real-time alters to the headteacher/Deputy Headteacher to action when an inappropriate use has been logged on a device. Should an adult in school identify an inappropriate use of a device the Online Safety Incident Flowchart (see below) should be followed, this gives clear systems and processes to follow when an inappropriate use has been identified.

We will also monitor the use of technology by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor pupils, and where necessary, support individual pupils where they have deliberately or inadvertently been subject to harm.

As part of our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, we have a duty set out in the KCSIE

framework to do all that we reasonably can to limit children's exposure to risks from the school's IT system. As part of this process, we have appropriate filtering and monitoring systems (Smoothwall monitoring) in place and regularly review their effectiveness. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.



(SWGfL Online Safety Group)

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures and logged on Arbor under the school's behaviour management monitoring system.

As part of this duty, we ensure we:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet children's safeguarding needs.
- That the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- That all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Appendix 1
St Edward's Computing and Online Safety Promise

To keep me safe whenever I use the internet, I promise…

- to keep my username and password private and not to use anyone else's
- to keep all personal information private like my name, address, school, date of birth, usernames and passwords along with other important information

- to block unknown links and attachments by not opening anything that I do not trust and to ask an adult straight away if I am not sure

- to report any messages or internet pages that are unsuitable or upsetting to an adult
- to tell an adult I trust like my parents or a teacher if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked.
- I will not play games unless I have permission.
- I will not open, copy, delete or change anyone else's files, without their permission and will always check with an adult if I am not sure about something.
- I will not log into someone else's account without their permission.
- I will always tell an adult if I believe one of my passwords has been compromised so I can get a new one.
- I will be polite and think carefully about how I talk to others online and what I say about them – If I wouldn't like something in real life I won't do it online!
- I will not take, copy or send pictures of anyone without their permission.
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal.
- I will not try to get around the filtering or security systems.
- I will not install any programmes or change the settings.
- I will not use chat and social networking sites unless I have permission from a teacher.
- I will not copy other people's work and pretend it is my own.
- I will check that information I use from the internet is from a trusted website.

Appendix 2

ST EDWARD'S COMPUTING CURRICULUM - Content, Contact, Conduct and Commerce

FS

FS children have access to the online world through chromebooks and tablets within their setting. Children are taught how to be safe throughout the school year when using these devices and are supervised when doing so.

Year 1

• Knows how to be safe, responsible and respectful online.	CONDUCT/ CONTACT	Children need to know how to behave in a manner that keeps them safe. They also need to know who it is okay to talk to online and what things are okay to share online.
• Knows to tell an adult when they see something unexpected or worrying online.	CONTENT/ CONTACT	Children need to know to tell a trusted adult and that this applies in home and at school.
• Knows how to stay safe when visiting a website or app.	CONTENT/ COMMERCE	Children need to know to talk to a trusted adult and listen to the rules set by their teachers/adults in school or at home.
• Knows why it is important to listen to their feelings when using technology.	CONDUCT	Children need to understand that the online world is useful and can be helpful but that a balance is needed and to recognise how they are feeling and when to take a break. They also need to understand that their adults should help them to make this decision when they are young.
• Use links (Including favourites) to websites to find information.	CONTENT	Children need to understand that they should only use the links provided and approved by their trusted adults and that this will help to keep them safe.

Year 2

• Know how to be a good digital citizen.	CONDUCT/ CONTACT	Children need to know what behaviours are appropriate online and what behaviours are not. They also need to know what they can share and who they can share it with when working online.
• Know what kind of information should be kept to themselves when using the internet.	CONDUCT/ CONTACT	Children should be aware of what is classed as personal information and that they keep personal information private. They also need to understand that they should seek support from a trusted adult if they are ever asked to share this information or if they accidentally share this information.
• Know what information is okay to have in their digital footprint.	CONDUCT	Children should be aware of what they should be sharing online and also what to do if they are unhappy about something that may have been shared about themselves via someone else.
• Know how we are all a part of an online community.	CONDUCT/ CONTACT	Children need to understand the risks of talking to others when online and that people may not be who they say they are. They also need to understand that their behaviour and

		how they act towards others has an effect on the online community they are part of.
• Know what they should do if someone is mean to them online.	CONDUCT/ CONTACT	Children understand that they must tell a trusted adult if they are unhappy with the behaviour of others online and that it is okay to do so.
• Knows of at least one online tool where ideas can be shared with other people.	CONTACT/ CONDUCT	Children understand what information they can share with others online and know how to behave respectfully when sharing online.

Year 3

• Knows how digital citizens take responsibility for themselves, their community and their world.	CONDUCT/ CONTACT	Children know how to behave appropriately when posting online, what they can and can't share and the effects that this will have on others in their digital community.
• Know that what they post online can affect their identity	CONDUCT/ CONTACT	Children know what material is appropriate to share with others online and what should be shared with them. They share an understanding that their digital footprint can be difficult to remove once information has been shared.
• Knows what makes a strong online community.	CONDUCT/ CONTENT/ CONTACT	Children understand who safe people to contact digitally are and what information they should share/keep private. They understand who to talk to if they are unhappy or worried (trusted adults) and know when to seek help on the behalf of others.
• Knows what they should do when someone uses mean or hurtful language online.	CONDUCT/ CONTENT	Children understand to talk to a trusted adult if they are unhappy.
• Understands why people alter digital photos or videos.	CONTENT	Children show an awareness of online information not always being true and some of the reasons why people may choose to alter images/information.
• Use an appropriate tool to share my work online	CONDUCT/ CONTACT	Children listen to their teachers and follow instructions when sharing information online. They know to use approved platforms and what information they should share/keep private.
• Use search tools to find and use an appropriate website	CONTENT	Children understand how a search engine works and will be mindful of the links they are clicking on. They understand what to do if they are unhappy with any content in search results and report this to a trusted adult.
• Knows different ways to communicate with others online	CONTACT/ CONDUCT	Children understand that there are different ways that they can communicate online but that their safety remains the same throughout these platforms as does the information they should/should not be sharing.

Year 4

• Knows what makes a healthy media choice.	CONTENT	Children understand what content is appropriate for their age-range and understand that rules are put into place for their own safety. They also understand that

		they have a responsibility for their own safety as well as their trusted adults.
• Knows what information about themselves is ok to share online and understands why passwords need to be secure.	CONDUCT	Children understand how to create a strong password to keep their personal information private and know that this should not be shared with others.
• Knows how their online activity affects the digital footprint of themselves and others.	CONDUCT	Children are aware that their digital footprint is everything they do or share online and that if they share information about others they are also affecting their digital footprint. Children understand the difficulties with removing information from online once it has been shared and therefore know why it is important to behave sensibly and safely.
• Knows how to be positive and have fun whilst playing online games and how to help others do the same.	CONDUCT/ CONTACT	Children understand that they need to be kind online with others and that they should report unkind behaviour/words to their trusted adult.
• Can talk about why an adult should be consulted before downloading files and games from the Internet.	CONTENT/ COMMERCE	Children understand that downloads can contain viruses and that this can have an effect on their hardware/software. They also understand the risks with downloading unknown material that may not be what it seems (inappropriate)
• Knows how to be upstanding when they see cyberbullying.	CONDUCT	Children know how to support others who may be experiencing unkind/unsafe behaviour online. They understand that sometimes they may have to report something on behalf of someone else.
• Use an appropriate tool to share my work and collaborate online	CONDUCT/ CONTACT	Children know which apps/platforms are safe for them to use and know to double check with a trusted adult if they are not sure. Children can share their work safely and conduct themselves sensibly when working collaboratively online.
• Identifies key words to use when searching safely online.	CONTENT	Children understand that search engines in school have a safe search filter to keep them safe and that search engines at home may not have this feature. They know to report any inappropriate material in school or at home to a trusted adult.
• Create a hyperlink to a resource online within their own work.	CONTENT	Children only use links to websites they know are safe and appropriate to others. They do not visit unknown websites via links nor do they link inappropriate sites in their own work. They understand that if they are not happy they can report to a trusted adult.

Year 5

• Knows what clickbait is and how to avoid it.	CONTENT COMMERCE	Children understand that some adverts are placed to encourage people to visit sites they would not usually visit and that sometimes this can encourage pop ups and viruses onto devices. They know that the information is not always the truth and that sometimes is can be inappropriate. They know what to do if they are unhappy with anything they see online.

• Understands how gender stereotypes shape their experiences online.	CONTENT	Children understand that games and platforms etc do not have to be specifically aimed at certain genders. When children talk about genders during RSE as this often comes up it is important to remind them of the safety of looking up answers to questions as there could be inappropriate material – remind to ask a trusted adult.
• Knows how to keep online friendships safe	CONTACT CONDUCT	Children understand how to be safe online, how to keep their personal information private and to report anything they are unhappy about to their trusted adults/
• Knows what Cyberbullying is and what they can do to stop it.	CONTACT CONDUCT	Children understand that bullying/cyber bullying is unkind behaviour over a prolonged period of time and that cyber bullying is just as real as in person bullying. They understand who they can talk to to get help and they understand not to delete or get rid of any messages/pictures etc but to share them with their trusted adult.
• Understands what the important parts of an online news article are	CONTENT COMMERCE	Children understand that online news articles often have adverts within them and that these may lead to phishing scams etc. They know where to find reliable information regarding current news affairs.
• Select an appropriate online or offline tool to create and share ideas	CONDUCT CONTACT	Children know which platforms are safe to share their work on and know how to behave appropriately when creating content collaboratively.
• Review and improve their own work and support others to improve their work.	CONDUCT CONTACT	Children know how to behave appropriately when working with others and understand the importance of being kind and respectful. They know not to share personal information online.
• Use different online communication tools for different purposes.	CONTACT CONDUCT CONTENT	Children understand the risks with communicating online, know what information to share/keep private and are able to navigate sensibly and safely around approved online platforms.
• Use a search engine to find appropriate information and check its reliability.	CONTENT	Children understand that search engines sift through a huge amount of information and that not all of this information is appropriate or true. They know what to do if they are unhappy with anything they see online.

Year 6

• Knows how to communicate safely on the internet: focus on social networking, chatrooms, blogs and other online communication) www.thinkuknow.co.uk	CONTENT CONTACT CONDUCT	Children understand the risks in communicating with others online. They know who it is appropriate to communicate with and they know that not everyone is who they seem online. They understand what to do if they are unsure. They know what information to keep private.
• Can describe strategies for issues of personal safety online.	CONTACT	Children know what to do if they feel unsafe/unsure when chatting/working/playing online. They are proactive about their personal safety online.

• Is able to discuss and demonstrate good online etiquette.	CONDUCT	Children know and understand that their behaviour online should not differ from their real life behaviour in that they should use the same kindness they do face to face. They understand to tell a trusted adult if they or their friends are unsure.
• Understands the pros and cons (uses and misuses) of social media	CONTENT CONTACT CONDUCT COMMERCE	Children understand the age restrictions with social media platforms. They also understand how social media can affect a person's mental health. They know the positive and negative effects and feel confident in using this to inform their online experiences with social media as they grow older. They know who to report to if they are worried or unhappy.
• Select an appropriate tool to communicate and collaborate online.	CONTACT CONDUCT	Children are able to choose the best fit platform from the selections used in school and can confidently navigate them safely. They understand that their online behaviour reflects on their real life behaviour and they make sensible choices accordingly.
• Check the reliability of a website.	CONTENT	Children can use their knowledge of websites to check whether a site is reliable. They understand that not all information online is truthful and can check this against a range of other safe sources.