

St Edward's Primary School E-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.

St 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
- robust internet filtering
- 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.

Users are not allowed to:

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 monthly newsletters, Parent Forums and the school website and social media.

Monitoring

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.

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.

Appendix 1

St Edward's Computing and E-Safety Promise



ZIP IT

Keep your personal stuff private and think about what you say and do online.



BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

To keep me safe whenever I use the internet or email, 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 understand that if I use a general year group log in, the same rules still apply.
- 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 not try to download pirate copies of music, videos, games or other software.
- I will check that information I use from the internet is from a trusted website.

Appendix 2

E-Safety Curriculum

See long term plan and medium term plans for further detail on content.

Year 1

- Knows how to be safe, responsible and respectful online. CONDUCT/CONTACT
- Knows to tell an adult when they see something unexpected or worrying online. CONTENT
- Knows how to stay safe when visiting a website or app. CONTENT
- Knows why it is important to listen to their feelings when using technology. CONDUCT

Year 2

- Know how to be a good digital citizen. CONDUCT/CONTACT
- Know why it is important to have device free moments in our lives.
- Know what kind of information should be kept to themselves when using the internet. CONDUCT
- Know what information is okay to have in their digital footprint. CONDUCT
- Know how we are all a part of an online community. CONDUCT/CONTENT
- Know what they should do if someone is mean to them online. CONDUCT/CONTACT
- Know how to give credit for other people's work COMMERCE

Year 3

- Knows how digital citizens take responsibility for themselves, their community and their world. CONDUCT/CONTACT
- Knows how a strong password can help to protect their privacy.
- Know that what they post online can affect their identity. CONDUCT/ CONTACT
- Knows what makes a strong online community. CONDUCT/CONTENT/CONTACT
- Knows what they should do when someone uses mean or hurtful language online. CONDUCT/CONTENT
- Understands why people alter digital photos or videos. CONTENT

Year 4

- Knows what makes a healthy media choice. CONTENT
- Knows what information about themselves is ok to share online and understands why passwords need to be secure. CONDUCT
- Knows how their online activity affects the digital footprint of themselves and others. CONDUCT
- Knows how to be positive and have fun whilst playing online games and how to help others do the same. CONDUCT/CONTACT
- Can talk about why an adult should be consulted before downloading files and games from the Internet. CONTENT/COMMERCE
- Knows how to be upstanding when they see cyberbullying. CONDUCT/CONTACT
- Knows what rights and responsibilities they have as a creator. COMMERCE

Year 5

- Knows what media balance means to them. CONDUCT
- Knows what clickbait is and how to avoid it. CONTACT/COMMERCE

- Understands how gender stereotypes shape their experiences online. CONTENT
- Knows how to keep online friendships safe CONTACT/CONDUCT.
- Is able to discuss and demonstrate good online etiquette. CONDUCT
- Knows what Cyberbullying is and what they can do to stop it. CONTACT
- Understands what the important parts of an online news article are CONTENT.

Year 6

- Knows how to communicate safely on the internet (focus on social networking, chatrooms and other online communication) www.thinkuknow.co.uk
CONTENT/CONTACT/CONDUCT
- Can describe strategies for issues of personal safety online. CONTACT
Understands the pros and cons (uses and misuses) of social media. CONTENT/
CONTACT/CONDUCT/COMMERCE