St Martin's School
E-Safety Policy

Introduction

At St Martin's School we understand the responsibility we have to educate our pupils on e-safety issues, including the 4Cs' (content, contact, conduct and commerce); teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Internet Websites

- Access will be granted for all but must be age appropriate and used for educational purposes.
- Access will be filtered and monitored.
- Pupils, staff and parents informed of Internet monitoring.
- Rules for appropriate internet use will be posted in all classrooms.
- All pupils and staff sign an internet acceptable use policy annually.

School Website and media

- Home/personal info will not be published and pupil photos will not enable identification. Only pupil's first names used
- Pupil content requires parental permission and will be removed at parent's request.
- Copyright must be respected.
- Website complies with publishing guidelines

Complaints/Sanctions

- Staff to report any online safety concern following safeguarding procedures.
- Staff misuse must be reported to the HT.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school safeguarding procedures. Concerns over radicalisation/extremism are dealt with in accordance to our Safeguarding and Extremism and Radicalisation policies.
- Serious issues involve police contact.
- The school will work in partnership with all involved parties to resolve issues.
- Sanctions include: interview by HT; inform parents/carers; removal of access.

Email

- Access granted for all where appropriate but must be used for educational purposes.
- All users of school e-mail systems sign an acceptable use policy at admission.
- Accounts updated/tracked.
- Staff must report inappropriate e-mail
- External outgoing e-mail should be written carefully and, where necessary, authorised in the same way as an outgoing letter written on school headed paper would be.
- The forwarding of chain letters is not permitted.

Safety/Risk Management

- All reasonable precautions will be taken and risks reviewed regularly.
- Assessment of risk and educational benefit prior to pupil access.
- Partnership approach to ensure pupil protection is reviewed and improved.
- Virus protection installed and updated.
- Secure filters are installed which prevent children and adults from accessing and/ or sharing any extremist online materials.
- School/ISP cannot guarantee content.
- Clear procedures are in place should inappropriate website content/ emails occur – computers are physically closed but not shut down and it is reported to the Safeguarding Lead.
- Procedures set out in 'What to do if ...' document are shared annually with staff and displayed in the staffroom.

Teaching and Learning

- Clear, progressive online safety program forms part of the Computing curriculum. Skills and behaviours embedded in other appropriate curriculum areas (e.g. RSHE).
- Pupils taught - Effective Internet research - Copyright respect
- Instruction must precede access. Plans for internet use are age appropriate with clear objectives.

Parents/Carers

- A partnership approach is adopted including demos, practical sessions and suggestions for safe Internet use at home.
- Parents/Carers provide consent for pupils to use the Internet, as well as other technologies, as part of the acceptable use agreement form at time of their child's entry to the school (including use of photographs).
- Parents/Carers are informed of what constitutes misuse and what sanctions may result from this.

Staff

- Are provided with appropriate training.
- Sign acceptable use policy annually to accept terms of responsible internet use, which are displayed in the staffroom.
- Take responsibility for the safeguarding of pupils and follow appropriate procedures to report concerns. All are vigilant of radicalisation and extremism and equipped to follow correct procedures if a concern arises.
- Are informed of internet monitoring.
- Professional conduct is expected. This includes the use of social media outside of school.

The 4Cs of Online Safety

What are the online safety rules to follow?

In all four nations of the UK, online safety is part of the statutory safeguarding and child protection guidance for schools and colleges. This includes keeping children safe from harmful and inappropriate content online as well as being able to recognise concerns and take appropriate action.

In England, Keeping Children Safe in Education (KCSIE) is the statutory guidance for schools with the latest version in force from 1 September 2023.

The 4Cs of online safety

An important step in improving online safety at school is by identifying what the potential risks might be. KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract). These are known as the 4 Cs of online safety.

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

From https://learning.nspcc.org.uk/

During our Internet Safety lesson, E-Safety Days and Computing lessons, children are introduced to both the positive and negative elements of using the internet in children friendly language and explanations. All children are taught what they should do and who they should tell if they see or hear something on the internet that they do not like or upsets them.

Written by: Mr Lacey (Computing Lead)
Ratified by: Governors
To be reviewed: May 2025

Policy date: 29.01.24
Date: 19th February 2024