POLICY DOCUMENT	**Policy 2022**
STATUTORY	**Statutory**
Legislation: Education/Other	E-Safety
Lead Member of Staff	Rob Dell
Lead Board Member	Jacqueline Logue
Publication /Revision Date	January 2020
Approved by	Monthly Management Meeting
Approval Date	January 2022
Full Board Ratification Date	
Review Frequency	2 years
Date of next review	January 2024
Publication date: School Website Staff Information folder	January 2022
Chair of Board signature	

Rosemary Works School e-safety policy

Introduction

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

The purpose of this policy is to:

- To educate pupils about e- safety issues and appropriate behaviours so that they remain safe and legal online.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

Definition of Different Technologies

Website - a page or collection of pages on the World Wide Web that contains specific information which was all provided by one person or entity and traces back to a common Uniform Resource Locator (URL).

Email - messages distributed by electronic means from one computer user to one or more recipients via a network.

Instant Messaging - (IM) technology is a type of online chat that offers real-time text transmission over the Internet. A LAN messenger operates in a similar way over a local area network. Short messages **are** typically transmitted between two parties, when each user chooses to complete a thought and select "send".

Chat Room - an area on the Internet or other computer network where users can communicate, typically one dedicated to a particular topic.

Social Media - is computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is internet-based and gives users quick electronic communication of content.

Mobile Phones - a telephone with access to a cellular radio system so it can be used over a wide area, without a physical connection to a network.

Blog - a regularly updated website or web page, typically one run by an individual or small group, that is written in an informal or conversational style.

Downloading - is the transmission of a **file** from one computer system to another, usually smaller computer system. From the Internet user's point-of-view, to **download a file** is to request it from another computer (or from a Web page on another computer) and to receive it.

New Technologies

It is the responsibility of the senior management team, ICT lead and teachers to ensure they are aware of the latest technologies and social media platforms. The above terminology may change accordingly.

Pupils with SEN

Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties.
They have an increased risk of being bullied. Some pupils with SEN rely on adults to varying degrees, including personal care, and this vulnerability puts them at a greater risk of being harmed or abused.

Children with SEN at Rosemary Works School are protected with additional support from Teachers and Teaching Assistants to closely guide them through the use of the internet by working alongside them or adapting the relevant tasks appropriately according to their individual needs. These are included in the children's IEPs as relevant.

E-Safety in the Curriculum

Staff have access to 'Teaching Online Safety in School' DfE (June 2019) of which its main points are:

- It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app (page 6).
- However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils
- Schools can refer to the Education for a Connected World Framework for age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.
- When planning their curriculum, and how online safety fits within it, there are a number of areas we recommend schools consider, for example how to support vulnerable
- We recommend that schools embed teaching about online safety and harms within a whole school approach

Children are taught about e-safety according to what is age-appropriate content. We work closely with the NSPCC who advise us and the children annually on e-safety, the use of social media, cyberbullying and how to protect themselves. We also have an annual visit from the Metropolitan police who presents the Year 5 and 6 children with an internet safety talk and workshop. Whenever children use iPads or computers, they are reminded how to behave appropriately. The school uses fast broadband with appropriate filters to protect children from social media sites, inappropriate images and suspicious online searches.

This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example, citizenship education covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

How to evaluate what they see online

This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. We can help pupils consider questions including:

- is this website/URL/email fake? How can I tell?
- what does this cookie do and what information am I sharing?
- is this person who they say they are?
- why does someone want me to see this?
- why does someone want me to send this?
- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?

Online behaviour

This will enable pupils to understand what acceptable and unacceptable online behaviour look like. We teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

We help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
- looking at how online emotions can be intensified resulting in mob mentality
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and
- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

How to identify online risks

This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action. We can help pupils to identify and manage risk by:

- discussing the ways in which someone may put themselves at risk online,
- discussing risks posed by another person's online behaviour,
- discussing when risk taking can be positive and negative,
- discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- discussing the risks vs, the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

Reporting Incidents

All incidents must be recorded, dated and shown to the Senior Management Team. This information will be shared with parents and an appropriate plan will be put into place to safeguard all relevant individuals involved. Refer to the incidents flowchart on page 5.

Type of Incident

- bullying or harassment (cyber bullying)
- deliberately bypassing security or access
- racist, sexist, homophobic religious hate material
- Terrorist/drug/bomb making material
- Images involving abuse
- online gambling
- pornographic material

Parents' attention will be drawn to the school's e-Safety Policy in newsletters and on the school website. Parents have an online consent form they digitally sign upon enrolment at Rosemary Works to allow or disallow photos and videos of their children to be used within school, on our website and on our social media platforms which currently include Facebook, Twitter, Instagram and YouTube. All YouTube videos are unlisted and meet the regulations set out by YouTube.

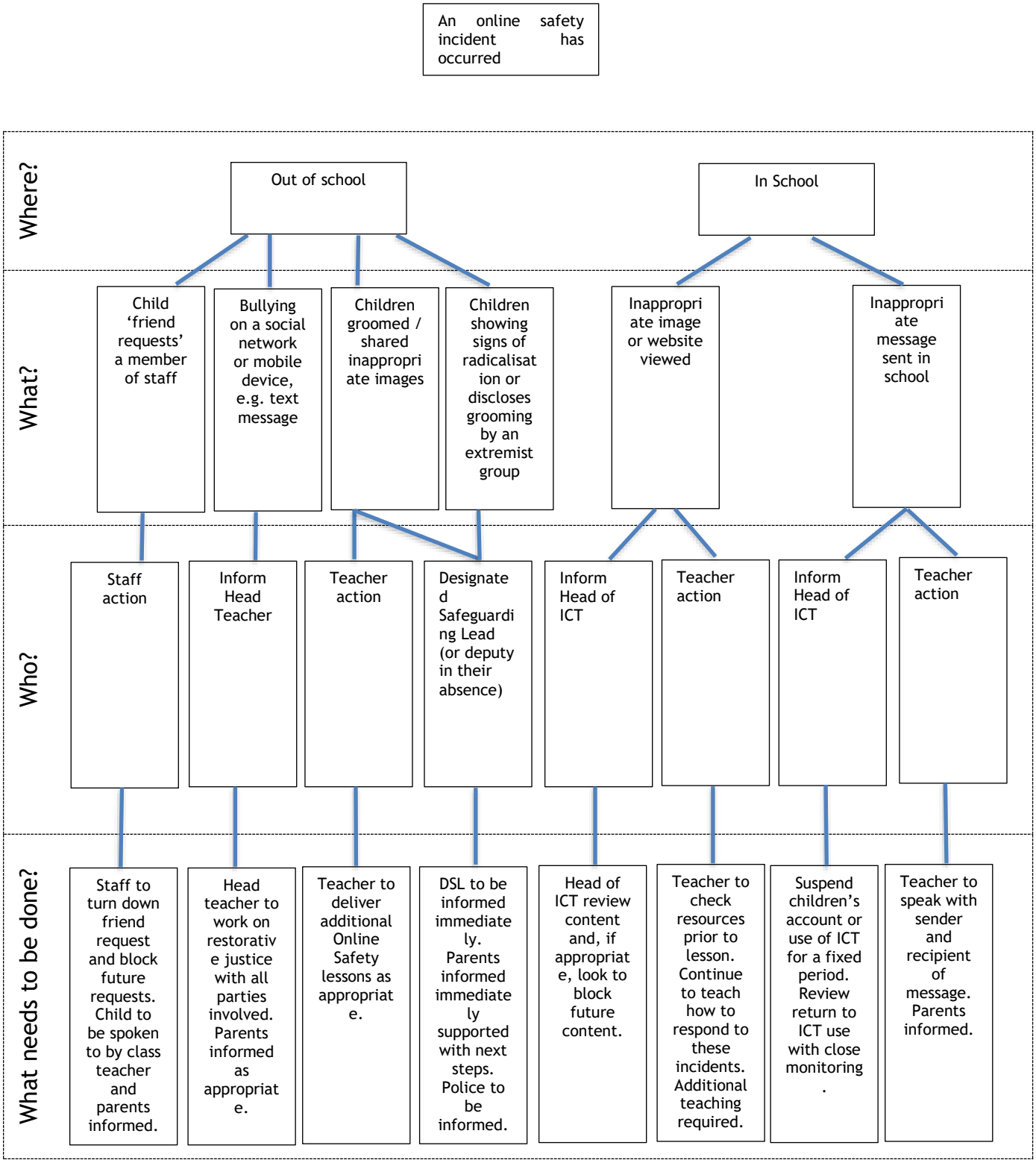
Email

Children at Rosemary Works, from Year 2 to Year 6 have school email accounts (name@rosemaryworks.com) in light of home learning due to the coronavirus global pandemic. These email accounts are accessed via Google and are managed and monitored by the DSL and are predominantly used for children to access Google Classroom and Seesaw during lockdown.

Passwords and Password Security

Children have supervised access to iPads and laptops in school. None of them are password protected, however our website, social media platforms and staff emails are secured using two step verification.

In the event of an Online Safety incident, follow this flowchart to identify what actions should be taken and by whom.



To ensure that members of staff are fully aware of their professional responsibilities when using information and communication systems equipment staff are asked to sign this code of conduct. Members of staff must read and understand the school's e-safety policy prior to signing.

I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises.

I understand that it is a disciplinary offence to use any school ICT system or equipment for a purpose not permitted by its owner. The Head Teacher will provide clarification.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email and social networking. ICT use may also include personal ICT devices with the permission of the Head Teacher if used for school business.

I understand that school information systems and equipment may not be used for private purposes without permission from the Head Teacher.

I understand that my use of school information systems, Internet and email is monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose or share any password or security information to anyone other than the Head Teacher.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding the inappropriate use of ICT systems or equipment to the Designated Child Protection Officer or Head Teacher.

I will ensure that all electronic communications that I make are compatible with my professional role.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Personnel responsible for overseeing e-safety in school: Rob Dell (Head Teacher) & Joseph Hughes (ICT Lead)