KINGSGATE SCHOOL

Document Type:	Guidance
Quality Standard	Protection of Children
Document Title:	**E-SAFETY STRATEGY GUIDANCE**
Date Issued/Review:	03.09.2018 / 03.09.2020 / 20.09.2021/ 26.09.2022/ 5.09.2023
Date of Next Review:	September 2024
Policy Owner:	Tim Rogers
Version Number:	1.3

CONTENTS

E-SAFETY STRATEGY GUIDANCE

1.0 INTRODUCTION AND DEFINITIONS

The rapid growth of the internet and of electronic technologies has opened up a world of exciting opportunities for children and young people. Through the internet and mobile technology it is possible for young people to have access to almost unlimited information worldwide, to be entertained with films and music and, through social networking sites, to contact and socialize with other young people. However alongside the benefits there are also risks and, while many young people are very competent in using these technologies, their knowledge and understanding of the risks is often very low.

The risks to children and young people are various:

- being exposed to inappropriate content;
- being groomed by someone who wants to abuse them;
- being bullied online or via mobile technology;
- being blackmailed;
- having their identity stolen; and
- being the subject of fraud.

Children and young people need to be protected from these risks and they need to be helped to develop the skills to keep themselves safe when they are online.

Four Cs that may present risks to children using technologies:

- **Content**: children may be exposed to inappropriate content which may upset or embarrass them, or which could potentially lead to their involvement in crime and anti-social behaviour.

- **Contact**: some people use the internet to groom children with the ultimate aim of exploiting them sexually. ICT offers new weapons for bullies who may torment their victims, for instance using websites or text messages. Social networking sites bring e-safety challenges, with many young people making available on linesome detailed – and sometimes inappropriate – personal information, which againraises both content and contact issues.

- **Commerce**: while the internet offers new opportunities for doing business online, it also brings with it many unscrupulous traders to whom children and young people may be particularly vulnerable.

- **Culture**: bullying via websites, mobile phones and other forms of communication device. Downloading of copyrighted materials e.g. music and films.

(Becta (2008) Safeguarding Children in a Digital World). Becta is the government agency leading the national drive to ensure the effective and innovative use of technology throughout learning.

1.1 On Line Grooming

> "*A course of conduct by a suspected pedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes*"

A full definition of Online Grooming can be found in the Sexual Offences Act 2003

Since the advent of the Internet, few internet forums have triggered such expressions of public concern for the welfare of young people as social network services (SNS). Despite the fact that online social networks have utterly revolutionised social interaction, this new environment can facilitate new forms of social deviance and criminality. Its ability to break down the conventional social barriers that govern sexual behaviour has compounded this situation, presenting new opportunities for sexual expression and deviance both to young people and to adults with a sexual interest in this group. This has resulted in a very real series of risks to the welfare of young people that socialize in this environment

> "The emergence of these superior communicative technologies, particularly social networking forums, has worsened the ability of those with deviant sexual fondness to communicate with persons who share similar interests throughout the world (Durkin and Bryant, 1995) and has enabled individuals with a sexual interest in children to access and engage directly with a pool of potential victims on an unprecedented scale. The types of interaction now possible present new opportunities to deviants to nurture and advance their sexual interests by observing and interacting with young people online, accessing erotic paraphernalia (text, images, video, live-time communication, etc.) and more ominously, soliciting direct engagement with children offline. The concerns have been reflected in a steady increase in the number of reports to law enforcement in the UK that relate to the sexual abuse of children and young people in social networking environments" (The CEOP Centre, 2006).

The e-safety strategy is designed to recognise that being safe online is not simply a matter of technology and that a comprehensive approach to e-safety is necessary, in which children and young people are kept safe by policies and practices that inform technical standards, alongside a programme of education for them and their carers/teachers which develops and sustains safe online behaviour.

The strategy has 4 strands:

- Infrastructure;
- Education;
- Supervision & Monitoring; and
- Acceptable Use Policies.

2.0 INFRASTRUCTURE

Access to the internet needs to be through equipment and connections that will allow for a good level of protection, filtering, and adult control.

2.1 Location of Internet Access

Internet access points in the school should be sited in communal areas that allow for reasonable oversight and monitoring of young people's use.

2.2 Security Software

Every school should review the security software currently available and ensure that suitable security is installed to reduce the risk of virus, Trojans, adware and cookies.

2.2 Age Related Filtering and Blocking

Schools will need to establish their own filtering and blocking criteria - each establishment must determine which sites they will block and which sites will be allowed to be viewed by certain age groups.

2.4 Spam Filtering and Blocking

Every school site should use effective filtering / blocking systems.

3.0 EDUCATION

Technical measures alone will not keep children and young people safe. There also needs to be comprehensive education and training for young people and for staff to learn about the risks of the internet and about the behaviours that are needed to stay safe online. The education of children and young people in developing the behaviours that will keep them safe when they are online is a key preventive measure. There needs to be an understanding that the propensity to engage in risky, sexually deviant behaviour is not just limited to predatory adults with a sexual interest in children. The accessibility of social networking forums to young people combined with unparalleled levels of media literacy within this population mean that young people can readily use online environments as an alternative social medium. Additionally, traditional social theory dictates that young adolescents engage in an exceptional level of socially disapproved behaviours that pose risks to their long-term well-being (Arnett, 1999), it follows that young people can and will exploit social networks to socialize, express themselves and experiment sexually; to behave and misbehave just as they would in real-world social environments.

3.1 Education for Children and Young People in School

Schools should ensure that e-safety is addressed through the PSHE curriculum.

3.2 Training for Staff

All staff will be provided with access to information and training resources about e-safety. This will include raising their awareness of the LSCB e-safety strategy in the geographical area in which their service is located, and understanding how e-safety relates to other company policies such as safeguarding and bullying.

4.0 SUPERVISION AND MONITORING

Once e-safety measures are put in place it will be necessary to monitor their effectiveness and be prepared to alter and update them as changes emerge in the internet.

4.1 Monitoring the Effectiveness of E-safety Measures

Each school must keep the effectiveness of its e-safety measures under review to ensure they remain ‘fit for purpose’.

4.2 Work with Children and Young People about Internet Safety

- Help children and young people to understand that they should never give out personal details to online friends they do not know offline.
- Explain to children and young people what information about them is personal: i.e. email address, mobile number, school name, sports club, arrangements for meeting up with friends and any pictures or videos of themselves, their family or friends. Small pieces of information can easily be pieced together to form a comprehensive insight into their lives and daily activities.
- Ensure children and young people are aware that they need to think carefully about the information and pictures they post on their profiles. Inform them that once published online, anyone can change or share these images of them. Advise them not to post any pictures, videos or information on their profiles, or in chat rooms, that they would not want a parent or carer to see.
- Remind children/young people who receive spam or junk email and texts, that they should never open them, or if they do, do not believe their contents, never reply to them or use them.
- Ensure that children and young people understand that some people lie online and that therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust.
- Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable.

4.3 Learning from Mistakes

In the event of breaches in internet safety (or 'near misses') schools must ensure that learning takes place to prevent a reoccurrence. Issues should be shared across the company to support opportunities for wider learning and the dissemination of best practice.

5.0 ELECTRONIC COMMUNICATIONS POLICIES

The Electrical Communications policy promotes responsible use of the internet by ensuring that users are responsible and safe, that they are not exposed to any damaging material and that systems are protected from accidental or deliberate misuse. They will apply to all staff using company IT systems, together with children and young people.

5.1 Staff will be Aware of the Electronic Communication Policy

All care and teaching staff will read and sign up to the company Electronic Communication policy.

5.2 Children and young people and the Electronic Communication Policy

Children and young people in education settings will have the local policy discussed with them, and will sign to confirm that they understand and agree to abide by it.

6.0 FURTHER INFORMATION AND RESOURCES

KidSmart is a practical Internet safety advice web site for schools produced by the children's Internet charity Childnet. The site focuses on five key SMART safety tips which children need to remember when they use the Internet. There are quizzes, lesson plans, resources, web

links, role play activities and PowerPoint presentations which can be downloaded. There are also free printed Internet safety leaflets and posters. http://www.kidsmart.org.uk
The **BBC** has produced guidance about using the internet in a safe way, with links to other useful websites with information for children and young people of different ages, parents, teachers and schools. http://www.bbc.co.uk/onlinesafety

Think U Know (www.thinkuknow.co.uk) website (developed by the police Child Exploitation and Online Protection Centre) alerts parents and children to Internet safety issues.

References

1. The company Electronic Communication Policy
2. The company Safeguarding Policy
3. The company Bullying Policy