Charlton Kings Junior School

Internet Safety/e-safety Policy

Governor Committee Responsible:	C&L	**Staff Lead(s)**:	Lauren John
Status	Statutory	**Review Cycle**	Annual
Last Review	October 2023	**Next Review Date**	October 2024

INTRODUCTION

The purpose of this policy is to make explicit the ways in which the Internet is used safely at Charlton Kings Junior School.

Aims for Internet Safety

To provide a learning environment with the highest standards of opportunity for children to achieve their full potential and as part of this aim we see access to the internet as a powerful tool.

We believe that access to the internet will:

- Enrich the quality of curriculum provision and extend learning activities
- Help us raise children's attainment
- Support teachers' planning and resourcing of lessons
- Enhance the school's management and administration systems
- Enhance staff development through access to educational materials, as well as the sharing of information and good curriculum practice between schools, support centres and educational authorities.

Legal framework

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- DfE (2023) 'Keeping children safe in education'

Inappropriate Material

Unfortunately, along with a wealth of useful educational sites on the internet, there are also sites which contain inappropriate materials which it would be unacceptable for children to gain access to.

To ensure that children access the internet within a safe environment, Focus Education provide us with our internet service, which is filtered by the SWgFL. This excludes unacceptable material through filtering lists of inappropriate sites to which access is barred when using the school's line. However, there is a very small risk that inappropriate material may occasionally get through unfiltered. As per KCSIE 2023, the DSL is responsible for ensuring the school has appropriate filtering and monitoring systems.

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the **DSL** will be informed and the police contacted.

E-safety education

An e-safety programme will be established as an integral part of the computing curriculum and other opportunities to re-inforce e-safety will be taught across the curriculum as opportunities arise, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.

As AI (artificial intelligence) becomes a greater part of internet interaction, the school will endeavour to teach children about the benefits and risks of this technology.

Clear guidance on the rules of internet use will be presented as part of the computing curriculum for each year group and reinforced regularly.

Pupils are instructed to report any suspicious use of the internet and digital devices.

PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

Children will be aware of and agree with the rules for responsible internet use as detailed in the pupil AUP – 'Think before you Click' (Appendix 1) before they are allowed access to the internet.

Children will be taught about using e-mail safely but will not send or receive e-mail at school.

Cyber bullying

For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHCE lessons as well as sex and relationship education.

The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our **Anti-Bullying and Anti-Hate Policy**.

Staff will:

- Take prompt action if they or their pupils encounter inappropriate material on the internet.
- Ensure children are shielded from unpleasant material (e.g. switch off the monitor and move children away).
- Inform the School Business Manager/Headteacher of any inappropriate site details as soon as possible.
- Discipline children if they make inappropriate use of the internet. (Sanctions should be in line with the school's Behaviour policy. The Headteacher should be informed of all incidents where a child has needed sanctioning for irresponsible use of the internet).
- Employ methods of good practice and act as role models for pupils when using the internet, including AI and other digital devices.
- Agree to, and comply with, the Staff IT Acceptable Use Policy.

Children should:

- Agree and follow the "Think before you click" guidelines (Pupil IT AUP).
- Inform a teacher immediately if they encounter any material that they feel is offensive or they think may cause offence to others.
- Be aware that their files held on the system may be reviewed by the teacher at any time.
- Be aware that they will incur sanctions if they make irresponsible use of the Internet.
- Not include personal details (e.g. address, 'phone number) on any communication system used at school.
- Respect copyright and acknowledge the source of material they have used from the Internet.

The school will:

- Inform all parents that their children will be provided with supervised Internet access as part of the school's curriculum.
- Internet access will be assumed to be authorised unless parents/carers inform us otherwise.
- Inform all parents of the school's "Think before you click" guidelines which their children will be expected to abide by in order to ensure a safe environment.
- Answer parents' queries and concerns about their child's use of the Internet and our safeguards to protect them from unpleasant material.

The school website

The school website provides information for parents, a showcase for school events, useful links for children, parents and teachers.