CAVERSHAM PARK PRIMARY SCHOOL

Online Safety Policy

Contents

Introduction

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

This Online Safety Policy outlines the commitment of Caversham Park Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

The Online Safety Policy has been written using statutory guidance from Keeping Children Safe in Education. This policy should be read alongside other relevant school policies and procedures, including:

- Safeguarding (including Child Protection) Policy
- Behaviour and Anti-Bullying Policies
- Code of Conduct for Staff and Volunteers
- Acceptable use of IT and Social Media Policy
- RSHE Policy

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- inform staff and volunteers with the overarching responsibilities, principles and procedures in managing online safety.
- Ensure that children should be able to use the internet for education and personal development, but that safeguards are in place to ensure they are kept safe at all times.

It is important to recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- Schools have a duty to ensure that all children, young people and adults are protected from potential harm online
- All staff and volunteers have a responsibility to help keep children and young people safe online, whether or not they are using the school's network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

<u>Responsibility and Monitoring:</u>

The Designated Safeguarding Lead takes lead responsibility (with the support of the Deputy Headteacher / Computing Leader; School Business Manager, the school's internet service provider, the schools IT technical support provider) for the areas of safeguarding and child protection within online safety including the filtering and monitoring systems and processes in place

The school will monitor the impact of the policy using

- *logs of reported incidents*
- *filtering and monitoring reports*
- *monitoring logs of internet activity (including sites visited)*

- *internal monitoring data for network activity*
- *surveys/questionnaires of: learners*; *parents and carers staff.*

Teaching and Learning

1.1 Why internet use is important

- The internet is an essential element of the 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- The internet is part of the statutory curriculum and a necessary tool for staff and pupils.
- Teachers plans develop internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum area.
- Staff model safe and responsible behaviour in their use of technology during lessons.
- Teachers remind pupils about their responsibilities when using the school network.
- Pupils use the internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

1.2 Internet use will enhance learning

- The school internet access is designed expressively for pupil use and includes filtering appropriate to the age of the children.
- Staff will guide pupils in on-line activities that will support their learning outcomes planned for the pupil's age and maturity.
- Pupils will be taught about acceptable use of the internet through the school's e-safety curriculum.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge of location, retrieval and evaluation as part of the school's computing curriculum.

1.3 Pupils will be taught how to evaluate internet content.

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught how to report unpleasant internet content to a responsible adult. This can be done anonymously, or in person, and will be treated in confidence.
- The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience. As part of this pupils will be taught to:
    - Understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour
    - know why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings
    - understand why they must not post pictures or videos of others without their permission.
    - understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
    - understand how search engines work and to understand that this affects the results they see at the top of the listings
    - be critically aware of the materials they read and be shown how to validate information before accepting its accuracy
    - understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - acknowledge the source of information used and to respect copyright when using the internet material in their own work

- know not to download any files – such as music files – without permission.
- develop strategies for dealing with receipt of inappropriate materials
- understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

Managing Internet Access

2.1 Information System Security

- The school computer system's security will be reviewed regularly under the guidance of the Headteacher, School Business Manager, Computing Subject Leader and the IT technical support service.
- Virus protection will be updated regularly on all school devices.
- Portable media must not be used by children without specific permission and followed by a security check.
- Security strategies will be discussed with the LA and the IT technical support service.

2.2 E-Mail / Direct messaging

- The personal e-mail addresses of staff and governors should not be used for school purposes. Personal email should be through a separate account.
- Access to school e-mail is at the discretion of the school and can be terminated at any time.
- Pupils are taught how to use email and direct messaging responsibly and how to report inappropriate/offensive content.
- Pupils may only use approved accounts on the school system and must only use these for school purposes.
- Pupils must immediately tell a teacher if they receive an offensive email or direct message.
- Incoming emails will be treated as suspicious and attachments not opened unless the author is known. Staff and pupils know that spam, phishing and virus attachments can make emails dangerous.
- Personal information about pupils must not be shared externally via email unless sent securely, e.g. password protected or encrypted.
- Any pupils or staff using offensive or bullying language or behaviour through e-mail will have their account terminated.

2.3 Published Content on the School Website / Online Platforms

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school website complies with the following statutory DfE guidelines for publications: What maintained schools must publish online
- Photographs published on the web do not have full names attached.
- The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

2.4 Publishing Pupil's Images, Videos and Work

- Digital Media that include images of pupils will be selected carefully so that individual pupils cannot be identified, or their image misused.
- Written permission from parents / carers will be obtained before photographs or videos of pupils are published online. Pupils' names will not be used anywhere on the website or

other online space, particularly in association with photographs or videos, unless consent has been granted.

- Effort is taken to ensure that pupils without photographic permission do not appear in group photographs. However, where this is not the possible, the photos will be edited to ensure that pupils without permission are not recognisable.
- Named pupils' work can only be published with the permission of the pupil and parents/carers.
- Access to the Foundation Stage Online Learning Journey is password protected. Parents / carers will be unable to download or save images from the resources and can only access information related to their child.
- Staff read and sign the school's Acceptable Use of ICT Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils

2.5 Social Networking and Personal Publishing

- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of most social network spaces are age restricted and that these are inappropriate for primary age pupils.
- Pupils will be advised to use nicknames and avatars when creating online personas.
- The Acceptable use of IT and Social Media Policy outlines guidance for staff and volunteers on using social media.

2.6 Managing Filtering

- The school will work with the IT technical support company and Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- User specific filtering systems are in place on all school devices.
- If staff, volunteers, or pupils come across unsuitable online materials, the site must be reported to the headteacher or Deputy Headteacher / Computing Subject Leader so that it can be reported and blocked. A log of incidents is kept by the school.
- The Headteacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Staff should not perform a search on a search engine (e.g. Google search) in view of the children without doing so prior to the lesson (in school) to check what results are drawn up.
- Teachers should ensure that children are not left to search the internet unsupervised and should check the sites that they plan to use with children prior to the activity.
- Children should not be left unsupervised at anytime whilst using the internet.

2.7 Managing the Emerging Technologies

- Emerging technologies will be examined for educational benefit and risks before use in school is allowed. Where necessary, a risk assessment will be carried out.
- The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

2.8 Protecting Personal Data

- The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.
- The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that

organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Policy Decisions

3.1 Authorising Internet Access

- All staff and volunteers must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff or pupils who are granted internet access. The record will be kept up-to-date: for instance, if a member of staff leaves or a pupil's access is withdrawn.
- Parents/carers will be informed that pupils will be provided with supervised internet access.

3.2 Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the International Scale and linked nature of the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will not accept liability for the material accessed, or any consequences of internet access.
- The school should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.
- The use of the computer systems without permission and for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

3.3 Handling Online safety Complaints

- Complaints of internet misuse will be dealt with by a member of the senior leadership team.
- Any complaint about misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and safeguarding policy.
- Pupils and parents/carers will be informed of the complaints procedure (see school's complaints policy).

3.4 Community use of Internet

- The school will liaise with local organisations to establish a common approach to online safety if necessary.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice, however they cannot be held responsible.

Communications Policy

4.1.1 Introducing the Online Safety Policy to Pupils

- This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum covering both school and home. This curriculum has been built around the materials available from 'Common Sense Media' and supported with other materials. Through this the Online Safety Policy is delivered to pupils.
- In addition to dedicated online safety lessons each half term, Online Safety guidance is also delivered through regular computing lessons and displayed in the computer suite.
- The school takes part in "Safer Internet Day" each year, during which age appropriate assemblies and lessons are carried out and pupils are taught about being safe online;

4.2 Staff and the Online Safety Policy

- All staff will be given the school Online Safety Policy.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and personal conduct is essential.

4.3 Enlisting Parents'/Carers' Support

- Parents'/carers' attention will be drawn to the school Online Safety Policy in newsletters and on the school website where appropriate.
- Online safety information sessions are held to inform parents / carers about the benefits and dangers of the internet and give them practical advice on how to protect their children.

5. **Online Risks**

- The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHCE) that some adults and young people will use such outlets to harm children. Posters providing information about how to get help are displayed around the school.

5. 1 Cyber bullying and abuse

- Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." – BullyingUK.
- Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.
- Through the PSHCE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

5.2 Sexual exploitation/sexting

- Sexting between pupils will be managed through our anti-bullying procedures.
- All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
- All incidents of sexting reported to the school will be recorded and referred to the DSL.

5.3 Radicalisation or extremism

- Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:
    - Encourage, justify or glorify terrorist violence in furtherance of beliefs.
    - Seek to provoke others to terrorist acts.
    - Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
    - Foster hatred which might lead to inter-community violence in the UK."
- The school understands that there is no such thing as a "typical extremist". Those who become involved in extremist actions come from a range of backgrounds, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

- The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.
- Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.
- Senior leaders will ensure that staff within the school complete regular Safeguarding training in the Prevent Duty.

Policy Date	Review Date
September 2023	September 2026