Castle School

E-Safety (Pupils)Policy

Status: Recommended	Drafted by: CCC ICT/C Rule	Date Approved: Autumn 22	Approved by: Head Teacher
Date to be reviewed: Autumn 2023	To be reviewed by: CCC ICT/ICT co-ordinator	Date shared with staff: Autumn 22	Publish on school website: Yes

Contents

E-Safety in schools is a safeguarding issue therefore this policy should be viewed alongside other Safeguarding policies including those for behavior, anti-bullying, personal, social and health education (PSHE), code of conduct and for citizenship.

1. Introduction

The purpose of this policy is to describe the safeguarding measures in place for adults and pupil in school:

- the ground rules we have developed in school for using the Internet and online technologies
- how these fit into the wider context of our other school policies
- The methods used to protect pupil from sites containing pornography, racist or politically extreme views and violence.

Ultimately, the responsibility for setting and conveying the standards that pupil are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At Castle School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

2. Rationale

In keeping with Castle School's vision for all our learners, this policy is based on

- *Respecting and valuing ourselves and others*
- *Having fun learning, playing and socialising*
- *Preparing for life in the wider community*
- *Aiming high and celebrating success*

2.1 At Castle school we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our pupils and staff must be able to use technology safely and effectively. The most effective way of doing this is to manage the risks rather than attempting to avoid them altogether.

2.2 The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. By supporting and educating our pupils we can support them to make safe decisions online when accessing technology inside and outside of school. Some of the dangers they may encounter include:

- Access to illegal, harmful or inappropriate images or other content

- Unauthorized access to / loss of / sharing of personal information
- The risk of being subject to grooming/radicalization by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

2.3 While pupils and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyber bullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision, to manage the risk and deal with any threat to safety.

3. Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.

Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the National Education Network (NEN) connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

3.1 When using online technologies, it is essential that pupils understand how to behave in a safe and responsible manner and how to react when faced with inappropriate content or situations which make them feel uncomfortable. At Castle School we believe that a comprehensive program of e-safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials from sites such as ThinkUKnow and ChildLine.

3.2 We believe that just as pupils learn how to swim by going to a swimming pool so they will learn safe life-long online behaviors by accessing and using the internet. Members of staff constantly monitor pupils' use of the internet and other technologies. Our program for e-safety education is evidenced in teachers' planning either as discrete or embedded activities. Messages involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Policies.

4. Information and Computing Technology in Castle school

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of this technology. This is provided and maintained by the Local Authority's Education ICT Service filtering services. Using the filtering service ensures we have an effective and secure system with firewalls to prevent staff/pupils or visitors from accessing extremist websites and materials in line with the PREVENT programme.

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and e-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

4.1 Technologies regularly used by pupils and adult stakeholders include:

Staff:

- Laptops and desktops – these should always be locked when staff are away from them.
- Cameras and video cameras, visualizers
- Internet, E-mail, *Office 365 and MS Teams*, central hosting including access to SIMS and confidential pupil information
- iPads, tablets
- mobile phones

Pupils:

- Laptops and desktops –
- Visualizers
- Internet, *office 365 and MS teams*, *zoom,* discussion forums, blogs and other communication tools – These may well be accessible at home
- Other peripherals such as programmable toys, control technology equipment
- iPads, tablets
- mobile phones

Others on school premises:

- Limited access to school systems such as filtered internet access using a visitor login.

4.2 Whilst we recognise the benefits of individual pupil logins to our school network, in KS1 and KS2 we prefer to use class logins for ease of access. As pupils move into KS3 they will then start to use individual logins. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the ICT service and key staff (Deputy Head, Business Manager, Office Manager and e-safety co-ordinator). School staff and pupils are **not** permitted to connect personal devices to the school's wireless network and the wireless key is **not** given to visitors to the school unless agreed by the Deputy Head.

5. The E-Safety Curriculum

We have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies In line with recommendations in the ESafety briefing for Ofsted Inspectors (Sept 2012).

These opportunities include:

- Termly Key stage assemblies
- Specific activities during E-safety day traditionally held in February and Anti-bullying (Friendship) week held traditionally in November
- Age-relate classroom activities using the ThinkUKnow and Childnet materials
- Specific targeted work relating to concerns or issues identified by school staff or parents
- ACE accredited scheme for pupils
- Related work in PSHE lessons
- Posters and reminders in and around the school
- Posters displayed by computers giving a summary of guidelines for safe internet use.
- Work requiring internet research or searching for pictures for a piece of work. Opportunities to discuss appropriate search terms. This is across all subject areas and encourages effective use of technology.

6. Safeguarding Staff and Children Online

6.1 Our School recognizes that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

> *Equip children to deal with exposure to harmful and inappropriate content and contact and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.*
>
> *UKCCIS (The UK Council for Child Internet Safety) – June 2008*

6.2 The school has published Acceptable Use Policies for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should the rules be broken.

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Coordinator/*Deputy Head* for investigation/ action/ sanctions.

There are different levels of access to the Internet for staff and pupils designed to protect everyone. For this reason, staff should never leave their computers unlocked when they are away from them, or give anyone else their password, or allow a child to use a computer using their account. The Internet service is filtered through the Meraki filtering service, provided by the ICT Service

6.3 Parental support for the E-safety policy.

The policy will be available to Parents on the website. Advice from school is always available and appropriate responses can be arranged. E.g. Information about Xbox parental controls.

7. Responding to Incidents – (Education Child Protection Service – June 2010)

7.1 It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to e-safety incidents are consistent with responses to other incidents in school. This may mean that serious actions must be taken in some circumstances. See below.

7.2 If an e-safety incident occurs Castle School will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs). Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

8. Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately to a member of the safeguarding team. It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented u**si**ng My Concern online.

Depending on the judgements made at steps 1 and 2 the following actions should be taken by the safeguarding team:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your Human Resources (HR) provider and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff.

9. Terms used in this policy

AUP: Acceptable Use Policy.

A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.

E-safety: We use e-safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that pupil may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting e-safety risks based on a combined approach to **P**olicies, **I**nfrastructure and **E**ducation, underpinned by **S**tandards and inspection. Whilst not explicitly mentioned in this policy, this model provides the basis for the school's approach to e-safety.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the pupil and young people in their care.

Schools: For ease of reading we refer predominantly to schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding pupil and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

The development of our safety policy involved…

- Carol Rule – ICT Co-Ordinator
- Anne Haberfield – Deputy Head Teacher
- Peter Nelmes – Senior Teacher – Therapeutic school lead

It will be available on the school website, MS teams and by request to the school office.

Relevant documents /Cross references:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Behaviour policy
- Safeguarding and Child Protection
- SRE (Sex and Relationships Education)
- PSHE Policy and Scheme of work
- Safer Working Practices
- Data Protection Policy
- County guidance (e.g. Use of Digital Images, e-mail)
- Acceptable use policy - AUPs- staff, pupil
- Anti-Bullying Policy
- School Complaints Procedure
- Cambridgeshire Progression in ICT Capability Materials – ICT services
- Risk assessment log
- Incident Log
- Keeping Children Safe in Education
- Code of Conduct