Paston Ridings Primary School

Online Safety Policy

Status	Statutory
Date approved	March 2021
Date of next Review	March 2023

Online Safety Policy

Contents

Background to this policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our approach to online safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- The Computing and PSHE Subject Leaders
- The governor responsible for Safeguarding

It was presented to the governing body on and ratified on 3rd *March 2021and* will be formally reviewed in March 2023

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email. and is readily available on the school network.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As Online safety is an important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale

At Paston Ridings Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '3 C's' **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming 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.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops, iPads and desktops - staff devices are also intended to be used off-site in accordance with the staff AUP, particularly with regard to GDPR.
- Some staff have access to school systems beyond the school building (e.g. MIS systems, Microsoft 365, Purple Mash).
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- Staff level internet access

Pupils:

- Curriculum laptops and iPads, including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources
- Purple Mash and other subject specific online tools providing pupils with access within and beyond the school gates

Where the school changes the use of existing technology or introduces new technologies, the balance of risks and benefits are always assessed. Where appropriate, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The online safety curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

At Paston Ridings Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool, so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

Our online safety curriculum is based on the Cambridgeshire Progression in Computing Capability Materials, and the Cambridgeshire PSHE Service Primary Personal Development Programme, with reference to UKCIS's Education for a Connected World

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online platform, Purple Mash. Purple Mash includes online safety curriculum materials which help to form the basis of our curriculum, alongside content from sites such as Project Evolve.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community
- A flexible curriculum which is able to respond to new challenges as they arise.

Continued Professional Development

Staff at Paston Ridings Primary School receive up-to-date information and training on online safety in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

New staff receive information on the school's online safety and acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Mobile phones and use of 3G and 4G data in school

In line with the Cambridgeshire and Peterborough Safeguarding advice, we take a cautious approach to pupil access to mobile phones and devices which allow for access to the internet through personal data plans. We have a policy for mobile phone use on school grounds. In particular:

- Pupils are dissuaded from bringing mobile phones to school. If it is deemed necessary for a pupil to bring a mobile phone to school, (e.g. in the case of older pupils because they travel to and from school independently), then the expectation is that the pupil hands their phone in to the school office on arrival.

Monitoring, and averting online safety incidents

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include secure, private CPSN provided internet connection provided by the east of England Broadband Network (E2BN), antivirus protection, managed firewalling and enhanced filtering provided by the Protex filtering system.

Staff also monitor pupils' use of technology and, specifically, the internet. Pupils' use of online services (including the World Wide Web) are supervised in school at all times. Staff use of the schools' internet can also be monitored and investigated where needed.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network.
- 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 school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case by case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

Responding to online safety incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, staff will follow the school's agreed procedures for responding, including internal sanctions and involvement of parents (this may include the deactivation of accounts, restricted access to systems, or reporting incidents to the police and other authorities – see flow chart below).

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

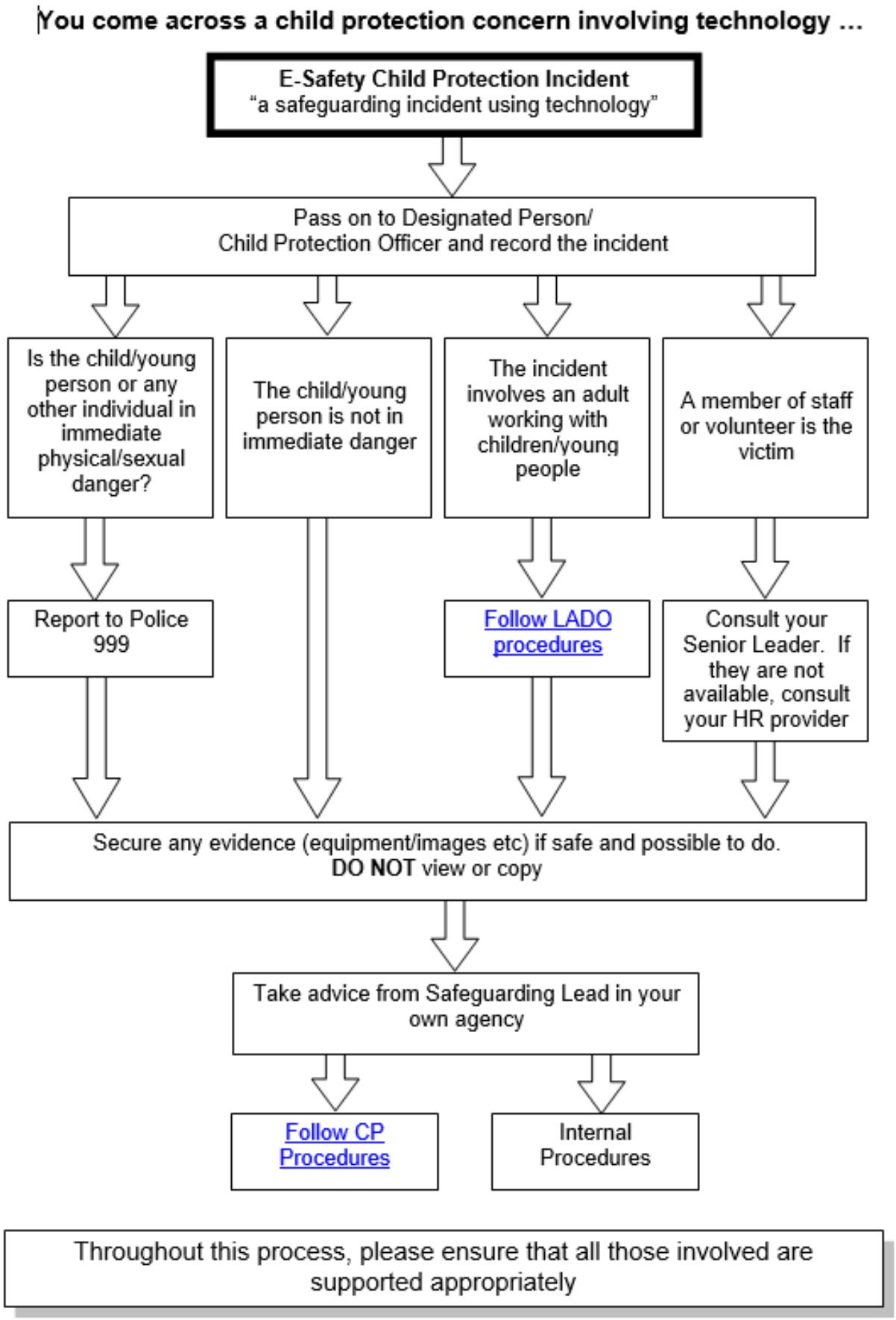
With this in mind, the headteacher may decide to take action in response to incidents which occur outside of schools if she deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action. In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Any necessary action will be taken in line with the DfE guidance on searching, screening and confiscation at school.

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.



Paston Ridings Primary School

E-Safety Incident Log

This form is only to be used to record online safety incidents which do not qualify as a child protection concern. Examples could include a child accidentally encountering inappropriate content when using a school device or minor conflicts between pupils as a result of interactions online.

Incidents which may be deemed a Child protection incident should be referred to the Designated Safeguarding Lead in the first instance, following the usual procedures.

If in doubt, consult with the DSL before completing this form.

Reported by: *(name of staff member)*	**Reported to:** *(e.g Headteacher, ICT Leader)*
Date:	**Date:**
Incident description: *(describe what happened, involving which children and / or staff, and what action was taken)*	
Review Date:	
Result of Review: *(any action taken)*	

Signature: (*Staff member dealing with incident)*	**Role:**	**Date:**
Signature: *(Senior Leader)*	**Role:**	**Date:**