# Fulbourn Primary School

# E-Safety Policy

*Document Number: FPS-POL-ESA-005*
*Body reviewed and approved by: Full Governing Body*
*Date adopted: 06 May 2020*
*Date for review (latest): May 2022*

# E-safety Policy

**Contents**

- The background to this policy
- Rationale
- The e-safety curriculum
- Continued Professional Development
- Monitoring, and preventing e-safety incidents
- Responding to e-safety incidents

**Background to this policy:**

The purpose of this policy is to describe the safeguarding measures in place for Fulbourn Primary School's staff and students, in school and at home, in relation to e-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 monitoring, and preventing and responding to e-safety incidents
- A progressive, age appropriate e-safety curriculum for all pupils

We define e-safety as the specific safeguarding issues that are associated with the use of technology, especially the internet. Therefore this policy should be viewed alongside other safeguarding policies including:

- Social Networking Policy
- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Data Protection Policy
- Anti-Bullying Policy

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

- This policy will be reviewed in response to specific e-safety incidents or developments in the school's use of technology. It has been shared with all staff via email and a staff meeting and is also available on the school network and website.

- Staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems. As E-safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteachers, the Designated Person for Child Protection and governors.

**Rationale:**

- At Fulbourn Primary School we believe that the use of technology in schools brings great benefits but we recognise that the use of these new technologies can put young people at risk within and outside the school.
- The school keeps children safe when using online technologies through a combination of:
  - e-safety education;
  - filtering and monitoring children's online activity;
  - reporting and responding to e-safety incidents that occur, including following child protection procedures where appropriate.

The risks children may face include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images, include those promoting self-harm or suicide;
- Loss of control of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing and distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication and 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 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.

E-Safety issues can also affect adults who work or are associated with the school.

Technologies regularly used by pupils and staff include:

Staff:

- Staff computers in classrooms, offices and the ICT Suite including staff level internet access and server access.
- Staff laptops can also be used at home in accordance with the staff AUP.
- Curriculum iPads for preparing and delivering pupil activities
- Class cameras and other peripherals such as visualisers and Interactive whiteboards

Pupils:

- Curriculum iPads, desktops in the ICT Suite and laptops for pupil use, which have filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, class cameras etc.)

**Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.**

**The e-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 National Curriculum for Computing states that:

- **At KS1:** use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Fulbourn Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. We follow the latest government guidance from June 2019, including use of *Education for a Connected World*, and we recognise that from September 2020, relationships education will be statutory. This subject will include e-safety messages.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is evidenced in teachers' planning.
- The Guide to Progression in Computing Document details the school's e-safety programme of study.
- Key e-safety messages are delivered and reinforced through whole-school participation in Safer Internet Day and other whole-school events, for example, assemblies during the year.

**Continued Professional Development:**

- Staff at Fulbourn Primary School receive up-to-date information and training on e-Safety issues in the form of staff meetings and updates from the Computing Subject Leader, as well as training from external providers where appropriate.
- New staff receive information on the school's acceptable use and Social Media policies as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

**Monitoring and averting e-safety incidents:**

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- Secure, private CPSN provided internet connection to each school with a direct link to the National Education Network. Managed firewalling.
- Restrictions on download of software, apps and file types from known compromised sites

Staff also monitor pupils' use of technology and, specifically, the internet.

Pupils' use of online services (including the World Wide Web) is supervised in school at all times.

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.
- 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 school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network.

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 reduce these risks to an acceptable level.

**Responding to e-safety incidents:**

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.

- E-safety incidents that have any safeguarding element are treated immediately as any other safeguarding concern and passed on to the designated person in school for child protection.
- If an e-safety incident occurs, Fulbourn Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).
- E-safety incidents that do not have a safeguarding component, for example when a child has been using the internet legitimately but has come across harmful or inappropriate content, may be referred to the computing coordinator and the ICT service, as appropriate.

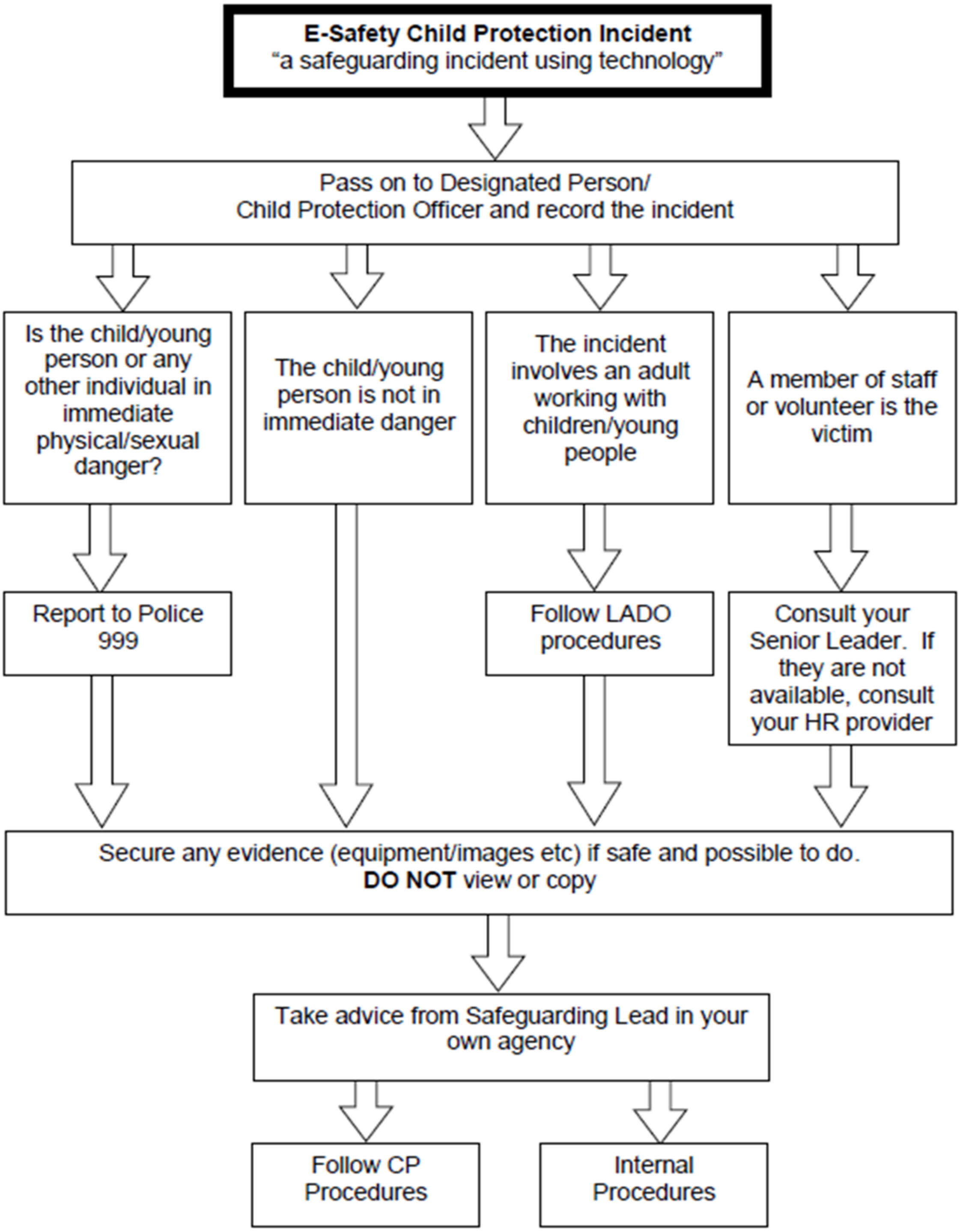
In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of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

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

**Summary**

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

**You come across a child protection concern involving technology …**



**E-Safety Child Protection Incident**
"a safeguarding incident using technology"

Pass on to Designated Person/
Child Protection Officer and record the incident

Is the child/young person or any other individual in immediate physical/sexual danger?

The child/young person is not in immediate danger

The incident involves an adult working with children/young people

A member of staff or volunteer is the victim

Report to Police 999

Follow LADO procedures

Consult your Senior Leader. If they are not available, consult your HR provider

Secure any evidence (equipment/images etc) if safe and possible to do.
**DO NOT** view or copy

Take advice from Safeguarding Lead in your own agency

Follow CP Procedures

Internal Procedures