# E SAFETY
# POLICY SUMMARY

## Learning, Developing, Growing Together

**Spinfield School**
**Terrington Hill**
**Marlow**
**Buckinghamshire**
**SL7 2RE**

**Tel: 01628 473551**
**Fax: 01628 477652**

| | |
|---|---|
| Updated: | March 2020 |
| Review date: | March 2022 |
| Signed: | |
| Position: | |
| Date: | |

# Spinfield Primary School
# E Safety Policy Summary

**Introduction**

The purpose of this Summary is to ensure that all staff, parents, governors and children of Spinfield School understand and agree the school's approach to e-safety. The summary relates to other policies including: E safety, Computing, Mobile phones and cameras, Bullying, Child Protection and Safeguarding and Health and Safety. A copy of the full E Safety policy provided by Turn it On can be provided on request.

**Writing and reviewing the e-Safety policy**

The school has a designated e-safety co-ordinator. The e-Safety policy has been agreed by the senior management team and approved by the governors. It will be reviewed every two years.

## Teaching and Learning

**The importance of internet and digital communications:**

The purpose of Internet access in Spinfield is:-

- to raise educational standards in all areas
- to provide pupils with access to the resources and information available world-wide through the Internet
- to support the professional work of staff
- to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and students.
It helps to prepare students for their on-going career and personal development needs.

It is a requirement of the National Curriculum (NC) orders for computing and is implied in other subject orders.

**Internet use enhances learning**
Internet access is provided by EXA and designed for pupils. This includes filtering appropriate to the content and age of pupils. Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirement. We currently use Purple Mash as our main provider for online learning and resources for the computing curriculum.

Pupils are given clear objectives and rules for Internet use and parents sign an Internet Code of Practice. Staff select sites which support the learning outcomes planned for pupils, age and maturity. Pupils are taught how to take responsibility for their own Internet access.

**Pupils are taught how to evaluate Internet content**
Pupils are taught ways to validate information before accepting that it is necessarily accurate. Pupils are taught to acknowledge the source of information when using Internet material for their own use. Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed. Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

## Managing Internet Access

**Information System Security**
School ICT system security is reviewed regularly. Virus protection is updated regularly. Security strategies are discussed with Turn it on and EXA

**E-mail**
Pupils email accounts are facilitated through the online learning platform, Purple Mash. Pupils can access this platform at home and are expected to use the same internet code of conduct that is taught in school. School e-mail accounts are only set up for pupils in Years 3-6 when permission has been sought by parents. Pupils must tell a teacher immediately if they receive offensive email. In computing lessons, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission. Pupils

are taught not to open suspicious incoming e-mails or attachments. The forwarding of chain letters is not permitted.

**Published content and the school web site**

The website complies with the school's guidelines for publications.

Pupils are taught to consider the audience and purpose for the work they publish on the school website and ensure their work is of high quality. Any work published on the website is checked by staff before uploading. All material must be the author's own work or, where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name. The contact details on the website are for the school administration only.

**Publishing pupils' images and work**

Photographs will not identify individual pupils. Group shots or pictures taken over the shoulder are used in preference to individual passport style images. Children's photographs are only allowed to go on the website once written permission has been received from the child's parents. Children's photographs are not accompanied by full names. Children's work which contains photographs must not contain the child's full name. Care must be taken to ensure that there is no other way the website can identify an individual pupil in a photograph - e.g. an article in the newsletter version shown on the website giving the name of a pupil with a related photograph elsewhere on the website.

**Social networking and personal publishing**

Pupils will not be allowed to access public chat rooms. Newsgroups are only available to staff. New applications will be thoroughly tested before pupils are given access.

**Managing filtering**

The school works in partnership with parents, the LEA, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Senior staff ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

**Managing video conferencing and webcam use**

During Video conferencing pupils must follow the school's Behaviour Policy. Video conferencing is always appropriately supervised and pupils must ask permission before accepting or making any calls.

Generally, video conferencing is planned for, and pre-arranged by, a member of staff.

**Managing emerging technologies**

Pupils are not permitted to use mobile phones during the school day. Children found with a phone will have it confiscated and parents contacted. If a child needs a mobile phone, they may give it to the class teacher who will store it safely until the end of the school day. The sending of abusive or inappropriate text messages, including sexting, is forbidden. Mobile phones must not be used during lessons by staff. They must be switched off. School photographs should not be stored at home.

**Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

## Policy Decisions

**Authorising Internet access**

All staff must read and sign the staff code of conduct for ICT before using any school ICT source. The school maintains a record of all staff and children who have access to the school's ICT system. Any person not directly employed by the school will be asked to read and sign the acceptable use of school ICT resources form before being allowed to access the internet from the school site.

**Assessing risks**

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the

school network. Neither the school, nor EXA can accept liability for any material accessed, or any consequences of Internet access. The school's E-safety Policy and its implementation will be monitored and reviewed on a regular basis.

**Handling e-safety complaints**

Complaints of internet misuse must be referred to the Headteacher. Any complaint about staff misuse must be referred to the Headteacher. If a complaint is made about the Headteacher, it should be referred to the chair of Governors. Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection Policy. Pupils and parents are informed of the complaints procedure. Pupils and parents are informed of the consequences for pupil misuse of the Internet

**Community use of the Internet**

The school liaises with local organisations to establish a common approach to e-safety and meet GDPR standards.

**Communications Policy**

**Introducing the e-safety policy to pupils**

E-safety posters are on display around school to remind pupils of their responsibilities and the Rules for Safe Internet Use

Pupils are informed that network and Internet use is monitored and appropriately followed up. The children receive e-safety lessons, appropriate to their age, and are constantly reminded of online safety. This is re-iterated at the beginning of each term.

**Staff and the e-safety policy**

All staff are trained regularly and receive a copy of the e-safety policy. Staff are informed that network and Internet traffic can be traced to an individual user. Staff will always use a child-friendly safe search engine when accessing the web with pupils.

**Enlisting parents' and carers' support**

Parents and carers attention is drawn to the school's E-safety Policy in newsletters and on the school website. The school has links on its website to e-safety resources. The school asks all new parents to sign

the pupil/parent agreement when they register their child with the school. The school regularly provides training for parents on internet safety.