# E-safety Policy

| | | | |
|---|---|---|---|
| **Date adopted** | September 2011 | **Owner** | Miss Lucy Groves |
| **Last reviewed** | September 2021 | **Review cycle** | Annual |

**Introduction**

This E-Safety Policy relates to other policies including those for Bullying and Safeguarding. The school E-Safety leader is Miss Lucy Groves. Our E-Safety Policy has been written by the school, building on best practice and government guidance.

**Links to Learning**

**Why internet and digital communications are important**

The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school Internet access is provided by Talk Straight via our IT support, Eduthing and includes filtering appropriate to the age of pupils at this school. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information appropriately to a wider audience.

**Pupils will be taught how to evaluate Internet content**

The schools will seek to ensure that the use of Internet derived materials by staff and pupils comply with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content in their computing lessons through Purple Mash online safety sessions.

**Managing Internet Access**

**Information system security**

Our ICT systems and security software are reviewed regularly. Virus protection is closely monitored and updated regularly.

**Emails**

Staff may only use approved email accounts on the school system for any matters relating to school. Incoming emails should be treated as suspicious and attachments not opened unless the author is known. All online activity will be closely monitored. The forwarding of chain letters is not permitted. Any emails to parents should either come from the school office account or be approved by a member of the ELT.

**Publishing pupil's images and work**

We do not post images of pupil's faces on media other than the school website (parents as asked to give us specific permission allowing this). Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name. The schools will seek to use group photographs rather than full-face photos of individual children. Pupil's full names will be avoided on the website, as appropriate, including in blogs, forums, or wiki pages, particularly in association with photographs. Written permission from parents/carers will be obtained before photographs of pupils are published on the school website. Parents are clearly informed of the school policy on image taking and publishing when they first register to the school in the registration and consent form.

**Social networking**

The schools filters access to social networking sites. Pupils will be taught 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 social network spaces outside school brings a range of dangers for primary aged pupils (through teaching, newsletters and our e-safety website page on the school website).

**Defining 'sexting'**
Whilst professionals refer to the issue as 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the internet'.

**Creating and sharing sexual photos and videos of under-18s is illegal.**
If a child within the school setting is involved with 'sexting' then the following procedures should be followed:

1. Do not view the imagery unless there is a clear reason to do so.
2. Refer immediately to a DSL within school with evidence.
3. DSL to discuss firstly with child, then parents/carers and if required to contact the police.
4. If the device needs to be seized and passed to the police then it should be confiscated, turned off and placed under lock and key by a DSL.

If children and parents follow our Mobile Phone Policy then this should not occur, as smart phones are not allowed in school. As per our policy, basic models, only under exceptional circumstances are allowed for children in Year 6 and should be retained in the school office during the day.

**Managing filtering**
The schools will work in partnership with Eduthing to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable online materials, the site must be reported to the E-Safety leader. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Mobile phones**
Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. It is strictly forbidden for both staff and visitors to use these devices to photograph children. Staff or visitors should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

Staff mobile phones should be switched off and left in a safe place during lesson times. Staff should only use mobile phones in areas where children are not present. Staff will use a school phone where contact with parents is required.

**Managing emerging technologies**
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. School cameras and tablet devices may be used within lesson time or for educational purposes only. The sending of abusive or inappropriate text messages is forbidden.

**Protecting personal data**
Personal data will be recorded, processed, transferred and made available in line with our Data Protections and GDPR compliance Audit.

**Wi-Fi**
The school Wi-Fi is only available for approved school and staff devices.

**Authorising Internet access**
All staff and visitors must read and sign the 'Acceptable Use Agreement/ICT Code of Conduct' (appendix 1) as part of their induction before using any school ICT resource, including the internet.

**Accessing risks**
The schools will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The schools cannot accept liability for the material accessed, or any consequences of Internet access. The schools will audit ICT use to establish if this policy is adequate and that its implementation is appropriate and effective.

**Handling E-Safety complaints**
Complaints of Internet misuse will be dealt with by a pupils class teacher in the first instance seeking support from a senior member of staff or DSL as appropriate. Any complaint about staff misuse must be referred to a Head of Schools or the Executive

Principal (if relating to the Heads of Schools) or the Chair of Governors if relating to the Executive Principal. Complaints of a child protection nature must be dealt with in accordance with our child protection policy and safeguarding policy.

**Community use of the Internet**
All use of the school Internet connection by community and other organisations shall be in accordance with the school E-Safety Policy.

**Introducing E-Safety Policy to pupils and parents**
Pupils and parents are annually asked to sign the e-safety advice page within the Handbook and Learning Dairy that each child is given at the start of the academic year. E-Safety rules will be discussed in classes at the start of each year and displayed in all classrooms (appendix 2). Pupils will be informed that network and Internet use will be monitored. Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils throughout the year.

**Staff and the E-Safety Policy**
All staff have access to this policy via our shared server. All Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

**Enlisting parents' support**
Parents' and carers' attention will be drawn to the school E-Safety Policy and advice in newsletters and on the school website. Parents and carers will, from time to time, be provided with additional information on E-Safety. The schools will ask all new parents to sign a parental consent form which confirms they have read and understood this policy, and give permission for their child to accent the internet at school within the policies guidelines.

## Appendix 1

Staff and Visitors

Acceptable Use Agreement/ICT Code of Conduct

**Introduction**
ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This Appendix supports our Staff Code of Conduct and is designed to ensure that all staff and visitors are aware of their professional responsibilities when using any form of ICT within a school setting.

- I appreciate that ICT includes a wide range of systems.

We expect all staff and visitors to:

- Understand that it is an offence to use a school ICT system for a purpose not permitted by its owner.
- Only use the schools' email/Internet/Intranet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Heads of schools or Governing Body.
- Comply with the ICT system security and do not disclose any passwords provided to me by the schools or other related authorities.
- Understand that I am responsible for all activity carried out under my username and will ensure that my computer is not left logged on when I am not in the classroom.
- To only use the approved, secure email system for any school business.
- To ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Heads of Schools or Governing Body.
- To not install any hardware of software without the permission of the E-Safety Leader.
- To not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Know that images of pupils will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent/carer. Images will not be distributed outside the schools' network/learning platform without the permission of the parent/carer or Heads of Schools.
- Understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager, or Head of Schools.
- To respect copyright and intellectual property rights.
- To not include children's names in e-mails or any other messaging.
- I will report any incidents of concern regarding children's safety to the E-Safety leader, the DSL or Executive Head Teacher.
- Lock all computers (click the windows key and L) when not in use.

Signature:

Date:

**Appendix 2**

This must be displayed prominently in each classroom

# E-Safety rules for KS2 Children
# Be SMART

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we not sure about.
- We only email people an adult has approved or through the learning platform.
- We send emails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open emails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We only use the school webcams when we are on a video call with another class or teacher
- We adhere to the remote learning guidance provided by the school

Class:

Date:

Signed by class teacher on behalf of the children:

This must be displayed prominently in each classroom

# E-Safety rules for KS1 and EYFS
# Be SMART

 **These rules help us to stay safe on the Internet.**

**We only use the internet when an adult is with us.**

 We can click on the buttons or links when we know what they can do.

We can search the Internet with an adult.

We follow the remote learning guidance. 

 We only use the school webcams when we are on a video call to another class.

We can write polite and friendly emails to people that we know and send them with teacher's permision.

We always tell an adult when we see something we are uncomfortable with on the internet.

Class:

Date:

Signed by class teacher on behalf of the children: