South Ossett Infants' Academy
E-Safeguarding Policy
September 2021

Introduction
ICT is an integral part of the curriculum at South Ossett Infants Academy. Our children have daily access to ICT and as 21st century learners, this will include access to the internet. The safety of all of our children is paramount and this document will outline measures which all stakeholders will put in place to ensure that our children remain safe while engaged in ICT based learning.

Aims

- To set out the key principles expected of all members of the school community at South Ossett Infants Academy with respect to the use of ICT based technologies.
- To safeguard and protect children and staff at South Ossett Infants Academy.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To equip our children with the knowledge and skills to enable them to use the internet safely under adult supervision both at home and school and keep parents informed about how we encourage safe use of the internet by our children.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with children.

Roles and Responsibilities

The Senior Leadership Team will ensure that:

- This policy applies to the whole school community, children, staff, parent helpers, students and the governing body.
- Mrs T Shute, head teacher, has ultimate responsibility for E- safeguarding. She will work closely with Lorraine Broadhead (ICT co-ordinator and designated person), who will attend ongoing training and network meetings to keep up to date with current practice.
- All members of staff, supply staff, students and parent helpers are made aware of the schools E-safety policy and protocols and will work to support and promote this policy.

The Governing Body will ensure:

- There is a senior member of the SLT who is designated to take overall responsibility on E-safety within the school.
- There is a system for incident reporting with procedures in place to deal with breaches of E-safety and security and that these incidents are logged.
- That staff have access to appropriate training where necessary.
- That they have read, understood and contribute to promote the school's E-safeguarding policy and protocols.
- Appropriate funding and resources are available for the school to implement their E-safeguarding policy.

- There is a web-filtering and monitoring system in place.

The Designated Senior Member of staff for E-safeguarding will:

- Act as first point of contact will regards to breaches in e-safety.
- Liaise with the designated Person for E-safeguarding as appropriate.
- Ensure ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and governors of the schools E-safeguarding policy.
- Ensure the school's ICT programs are reviewed with regard to security.
- Ensure that virus protection is regularly reviewed and updated.
- Ensure E-safeguarding is embedded across the curriculum.
- Ensure E-safeguarding is promoted to parents and carers.
- Ensure E-safeguarding log is kept up to date and regularly reviewed.

Teachers and support staff will:

- Read, understand and support the School's E-safeguarding policy.
- Read, understand and adhere to the school staff AUP (Acceptable Use Policy).
- Develop and maintain an awareness of current E-safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed E-safeguarding messages throughout the curriculum where appropriate.
- Supervise children carefully when engaged in learning activities involving technology.
- Be aware of what to do if an E-safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Managing Digital Content

- Parents are asked to sign a permissions form, which includes reference to use of digital images, audio and video.
- Children and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances personal equipment may be used with permission from the head teacher provided that any media is transferred solely to a school device and deleted from any personal devices.
- Digital images, audio and sound will be stored in the shared folder on the Schools main server and not in staffs own documents.
- Parents may take photographs at school events however, they must ensure that any images or videos taken, involving children other than their own, are for personal use and will not be published on the internet including social networking sites.
- Children will not bring their own mobile technology devices into school.
- Staff mobile phones are not taken into classrooms or areas where children are working except in exceptional circumstances and only with the agreement of a member of the SLT.

Teaching and Learning

In today's world, the internet and other technologies are embedded in our children' lives, not just in school but outside as well, and we believe we have a duty to help prepare our children to safely benefit from the opportunities the internet brings.

- Children are taught how to use the internet safely and under adult supervision; through regular E-safety discussions and assemblies, including the Smartie the Penguin presentation, supported by the "Think then Click" posters prominently displayed around school. When searching for images, sound and video children are directed to previously safely downloaded and stored data. When accessing the internet for material this is done under close supervision and is filtered by Smoothwall

- All adults sign an end-user Acceptable Use Policy (AUP) provided by the school. All users, in language appropriate to their age and access will be made aware that they must take responsibility for their use of and behaviour whilst using the school ICT system, and that such activity will be monitored and checked.

- E-safeguarding lessons are an integral part of the curriculum and are delivered in individual classes and assemblies as well as Internet Safety Week where appropriate. This is recorded in the E-safety log.

Passwords

- A secure and robust username and password convention exists for all system access (email, network access, school management information system).

- Users should change their passwords whenever there is any indication of possible system or password compromise.

- All staff will have a responsibility for the security of their username and password and must immediately report any suspicion or evidence that there has been a breach of security.

- Children will be taught about password security as part of E-safety discussions, assemblies and class teaching.

Filtering

- The school uses a filtered internet service. The filtering is provided through Smoothwall.

- The school's internet provision will include filtering appropriate to the age and maturity of children.

- If staff discover a website with inappropriate or illegal content, this should be reported to the E-safeguarding coordinator and the headteacher. All incidents should be documented.

- If users discover a website with potentially illegal content, this should be reported immediately to the E-safeguarding coordinator. The school will report this to appropriate agencies including the filtering provider.

- The school will regularly review the filtering product for effectiveness.

- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed for content prior to being released or blocked.

Internet access authorisations

- All adult users will sign an AUP provided by school.

- Foundation Stage and Key Stage 1 children's internet access will be directly supervised by a responsible adult.

Protecting Personal Data

- Staff will not remove personal or sensitive data from the school premises without permission of the Head teacher and without ensuring such data is kept secure.

- For further information see the Data Protection Policy.

- The Data Protection, Data Retention and Privacy Notices are available on the school's website.. are Privacy

E Mail

- Staff should only use approved email accounts allocated to them by the school for work related correspondence, and be aware that any use of the school email system will be monitored and checked.

- Staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.

Teams

- Teachers, practitioners and staff are given a Teams account with a password. For staff this is linked to their emails.

- The facilities of Teams, such as Teams Meetings, Files, Chat etc will be used to support Remote Learning and in addition to Parent Hub, to share and celebrate the children achievements including the posting of videos

- As well as sending home instructions on how to set up and use the Teams account, "Guidelines on how to use MS Teams" was also provided, to ensure Teams meetings are conducted safely and appropriately. This information is also on the website.

- The use of Teams and all Teams meetings are conducted in line with Safeguarding and E-safeguarding policies.

Emerging Technologies

This e- safeguarding policy takes account of technologies currently being used at South Ossett Infants Academy. As new technologies emerge and are adopted the policy will be reviewed and adapted where necessary to ensure safety for the school community.

Use of mobile devices

- Children are not permitted to bring mobile devices such as mobile phones, tablets, cameras I pods and games to school.

- Staffs are allowed to bring mobile phones on to school premises but these will be stored with personal belongings out of reach of children.

- No images or videos should be taken on mobile phones or personally owned mobile devices without a person's prior consent.

Camera and Images

- Any photographs, audio and video should be taken using school devices. All data will be stored in the shared folder and deleted from devices on a regular basis.

Social Networking

- School does not make use of blogs, wikis, podcasts or social networking to publish content online
- Staff using websites such as Facebook and Twitter will not bring the school or their own professional status into disrepute.
- Staff will not discuss professional matters on social media sites.
- The Parent Hub app is used to communicate with parents and carers. All images, or information shared on the app, are approved by the headteacher or another member of the SLT.

Support for Parents and Carers

- Parents/carers will be informed of the Schools E-safety policy through the website with paper copies available on request.
- Parents/carers are asked to agree and sign the permissions slip, which clearly states the protocols for using use of photographic and video images outside school.
- Information on E-safety support is disseminated to parents/carers at least annually and more often as school receives relevant updates
- There are links on the school's website to additional e-safety support such as Net-aware; parents are informed of these via Parent Hub or newsletters attached to Parent Hub messages

Reviewed by Headteacher and Teachers September 2021
Reviewed and approved by Governors October 2021

To be reviewed September 2024