



South Hykeham Community Primary School
Wath Lane, South Hykeham
Lincoln LN6 9PG
Telephone/Fax: (01522) 681919
Headteacher: Mr John Richardson BSc (Hons) P.G.C.E.

E-safety Policy

1. Background

1.1 Although the use of I.T. and the internet provide ever increasing opportunities for children and young people to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

1.2 Apart from the risk of children and young people accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways. Increasingly, bullying may be conducted on the internet through social media or by the use of text messages as well as 'stranger danger' which could potentially lead to 'grooming'.

1.3 E Safety is seen as a safeguarding issue and not a technological issue and it is vital that our school is aware of the risks that are associated with safety as well as recognising the benefits digital technologies can bring.

1.4 Primarily e-Safety is used to describe pro-active methods of educating and safeguarding children and young people while they use digital technology. In order for children and young people to remain safe we should educate them not only in the dangers but also inform them who they can contact should they feel at risk and where to go for advice while still promoting the many benefits of using digital technology, thereby empowering them with the knowledge and confidence of well researched good practice and continuing development.

2. Aims and outcomes

2.1 E-Safety concerns safeguarding children and young people in the digital world.

2.2 E-Safety emphasises learning to understand and use new technologies in a positive way.

2.3 E-Safety is less about restriction and more about education about the risks as well as the benefits so children can feel confident online.

2.4 E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school including an understanding of the dangers of cyberbullying.

Children's knowledge by the end of Year 6:

- Never give out personal details to online friends that you don't know offline.
- Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family. Small pieces of information can easily be pieced together to form a comprehensive insight into your personal life and daily activities.



- Understand what to share and how to share safely when communicating using I.T.
- Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.
- It can be easy to forget that the internet is not a private space, and as a result sometimes people engage in risky behaviour online. Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent to see.
- If you receive spam or junk email and texts, never believe the content, reply to them or use them.
- Understand that some people lie online and that therefore it's better to keep online friends online. Never meet up with any strangers without an adult that you trust.
- Don't forget, it is never too late to tell someone if someone or something makes you uncomfortable.
- Understand different ways and suggested ways of dealing with information that may be upsetting e.g. what to do if inappropriate pictures arise or hurtful messages are sent.

3 Use of technology in school

3.1 Benefits of using the internet in education include:

- Access to world-wide educational resources;
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support service, professional association and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfE
- Ability for parents to support child's home learning;

3.2 The school internet access will be designed expressly for pupils use and include filtering appropriate to the age of pupils.

3.3 Internet access will be planned to enrich and extend learning activities.

3.4 It should be remembered that digital technology reaches far and wide, not only computers and laptops, but consideration should also be given to technologies such as: tablets, mobile phones; Xbox; Playstations; and anything else which allows interactive digital communication.

3.5 Children will be reminded and involved in discussions about e-safety throughout lessons using technology.

4 Teaching and learning across the curriculum

4.1 At South Hykeham Community Primary School, e-safety lessons will be taught to all children from Foundation to Year 6. The age of the children will reflect the technologies, social networking sites and games being used.

4.2 E-safety will be taught as a series of lessons in line with the computing curriculum; it will also be reinforced and discussed in all computing lessons.

4.3 When using school technology (laptops, computers, iPads, cameras, DS, iPods and other technology based games) in other curriculum areas expectations of online safety and guidance will be reinforced.

4.4 At South Hykeham Community Primary School, e-safety will be promoted through competitions, displays, assemblies and through posters displayed on the iPad and laptop trollies.

4.5 Children will be made aware of the action to take if they find something that makes them feel uncomfortable or upset.



www.south-hykeham.lincs.sch.uk

E-mail: john.richardson@south-hykeham.lincs.sch.uk

4.6 Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use in school and guidance on out of school.

5 Passwords

5.1 Staff should keep passwords private. Passwords are confidential and individualised to each person.

5.2 Each child has their own username. Children should be taught about the importance of not sharing their passwords with children as we recognise that in the majority of cases children are taught the importance of sharing.

6 Data Protection

6.1 All sensitive data, such as children's details and reports, should be kept on the school network. Laptops/computers which can access the network are password protected.

6.2 Technology containing information about the school or children (for example, short term saving of reports to a pen drive) should be stored on a password protected device.

7 Images and Videos

7.1 Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent. If photographs are to be downloaded onto a personal computer staff must delete these once the child has left the school.

8 Mobile Phones

8.1 Staff should not use their personal phones for taking photographs. Each class and the school office have access to an iPad which will be used to take photographs.

8.2 Mobile phones should not be used when teaching, unless there are exceptional circumstances, but permission must be sought from the Headteacher.

9 Viruses and other malware

9.1 Any virus outbreaks are to be reported to the head teacher/computing co-ordinator as soon as it is practical to do so, along with the name of the virus (if known) so they are able to report it to the Ark technicians.

10 Logging concerns

10.1 Any concerns relating to safety are logged by the Headteacher and appropriate action taken.

11 Staff use of Internet

11.1 Use of the internet on school premises should principally be for school use, e.g. accessing learning resource, educational websites, use of email etc.

11.2 Staff should not be accessing the internet for personal reasons while teaching children.

11.3 Use of the internet to access any illegal sites or inappropriate material will be reported to the Headteacher and appropriate action taken (if accessed accidentally users should report the incident to the Headteacher as soon as possible).

11.4 The school recognises that many staff will actively use Facebook, Twitter (X), Instagram, Threads and other such social networking sites. Staff should not post material (including text or images) which damages the reputation of the school or which causes concern about their or any



www.south-hykeham.lincs.sch.uk

E-mail: john.richardson@south-hykeham.lincs.sch.uk

other member of staff suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.

11.5 It is never acceptable to accept a 'friend request' from pupils, as in almost all cases children of infant age using networks will be breaching terms and conditions of use of those networks. It is never acceptable to initiate a friend request with a pupil. It is inadvisable to accept friend requests from ex-pupils. It is inadvisable for staff to accept or initiate a friend request with a parent on social networking sites.

11.6 Setting a high security level on social networking sites is highly advised.

Signed Chair of Governors

Date: September 2023

Review: September 2026



www.south-hykeham.lincs.sch.uk

E-mail: john.richardson@south-hykeham.lincs.sch.uk