Ryhope Infant School Academy

E-Safety Policy

Updated:	March 2017
Produced by:	Ms S Reed Assistant Headteacher
Ratified by:	Governing Body – March 2017
Signed:	S. Brown Chair of Governors
Review Date:	March 2018

Rationale

Children and young people should have an entitlement to safe Internet access at all times. These e-safety guidelines should help to ensure safe and appropriate use of the Internet and related communication technologies. The use of these technologies can put young people at risk within and outside the school, however through good educational provision, we aim to build pupils' resilience to, and understanding of, the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The following risks have been considered:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the Internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / Internet games;
- 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 child/ young person.

Many of these risks reflect situations in the off-line world and the e-safety guidelines will be used in conjunction with the behaviour, anti-bullying and safeguarding policies. The e-safety guidelines that follow explain how we intend to help the children (and their parents) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope of the Guidelines

These guidelines apply to all members of the school community, including staff, pupils, volunteers, students, parents and carers, who have access to and are users of school ICT systems. They also apply to incidents of cyber-bullying, or other e-safety incidents within the terms of these guidelines, which may take place outside of the school, but are linked to membership of the school community.

The school will deal with such incidents within these guidelines and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Guidelines and for reviewing their effectiveness.

A member of the Governing Body has taken on the role of Safeguarding Governor including E-Safety and reports to the Governing Body. The current Safeguarding Governor is Ms S Brown.

The ***Headteacher*** has a duty of care for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety will be delegated to the Deputy Designated Safeguarding Lead, the School Business Manager and Curriculum Team Leaders*.*

The Headteacher:

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- provides advice for staff and others and organises training as needed;
- liaises with external agencies, particularly in respect of child protection issues arising from e-safety work;

The Deputy Designated Safeguarding Lead/E-Safety Lead:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety guidelines / documents;
- keeps up-to date with developments in relation to e-safety and disseminates these widely;
- helps ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- helps provide training and advice for staff and others;
- liaises with teaching and other staff in developing and evaluating e-safety educational programmes;

The School Business Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack, including regular updating of virus protection;
- that the filtering system provided by Advantex (Smoothwall) is applied effectively and consistently;
- that users may only access the networks and devices in line with the AUP

- that user names/access to school systems are updated e.g. when a member of staff leaves;
- that checks are carried out as required on staff laptops/ iPads;
- Liaises with technical support.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current e-safety guidelines and practices;
- they read, understand and sign annually to state they will follow the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Headteacher
- all digital communications are on a professional level and only carried out using official school systems*;*
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- personal data is handled securely (see e-mail and Data Protection sections below);
- pupils understand and follow the e-safety and acceptable use policies and have an understanding of digital literacy issues appropriate to their age.

Pupils (as appropriate for their age)

- become increasingly responsible for using the school ICT systems in accordance with the guidelines.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

Policy Statements

1. The importance of Internet use

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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. Because the Internet may be used within any curricular area and more widely within school, these E-Safety Guidelines should be adhered to at all times and within every aspect of school life.

2. Internet use to enhance learning

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

- Pupils are required to return a signed copy of the ICT Acceptable Usage Agreement for Pupils every year, which must be countersigned by their parent or carer (in the case of Foundation Stage, parental signature only required).
- 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, using a 'child-friendly' search engine eg *'Safe Search'*
- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited using a variety of approaches appropriate to the age and maturity of the children.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies and the internet.

3. Pupils will be taught how to evaluate Internet content/ Digital Literacy

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils are encouraged to tell a member of staff immediately if they find any material that makes them feel uncomfortable.
- Pupils are taught to question information before accepting it as true.

4. Educating parents and other carers

Parents and carers may not fully understand e-safety risks and issues, however they play an essential role in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, school web site
- High profile events / campaigns eg Safer Internet Day or school ‘E safety week’
- Reference to other relevant web sites / publications
- Other activities arising from parental suggestions or queries.

5. Education and training for staff

- A programme of e-safety training will be made available to staff including training as part of ongoing Safeguarding training. This will be regularly updated and reinforced.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety guidelines and Acceptable Use Policy.
- The Designated Safeguarding Leads (or other nominated person) will receive updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. These E-Safety guidelines and updates will be presented to and discussed by staff at least annually.
- The Designated Safeguarding Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

6. Governor education and training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways e.g:

- Attendance at training provided by the SSCB / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

7. Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number.
- Staff or pupils’ personal information will not be published.
- The Assistant Head teacher and School Business Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.
- All images of children will have no names attached. All parents are required to sign the Contact form annually to say that images of their children can be used.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of

those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed.

8. Social networking and Cyber-bullying

Staff follow the guidelines in the AUP. All staff are expected to have read and to abide by this. Failure could result in disciplinary action.

- The school will block/filter access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- The E-Safety Lead will aid staff in passing on relevant information to share with parents regarding the age restrictions/recommendations provided from safe sources linking to social media sites/apps.
- School will continue to find suitable, up to date resources to show the dangers of the use of social media to any child in the school – and the reasons for age restrictions/recommendations through specified workshops/activities and lesson ideas from schemes of work.
- Any incidents of cyber-bullying will be reported directly to the Designated Safeguarding Lead. Any outside agencies such as police etc will then be notified and child protection procedures will be followed. All incidents will be logged and regularly monitored, parents will also be informed.
- Other members of the school community affected by cyberbullying should also be supported by the school.

9. 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.

- Children are not allowed to bring mobile phones to school.
- Staff mobile phones are not to be used in the classroom during contact time.
- Staff cameras and other mobile devices are not to be used during contact time.
- School mobiles are available for Educational Visits.
- All staff, students and volunteeers are required to sign the schools Acceptable Usage Policy

10. Assessing risks

- Access to the Internet will be by adult demonstration with directly supervised access to specific online resources.
- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.
- The school will audit ICT provision to establish if the e-safety guidelines are adequate and that their implementation is effective.

11. Complaints

- Responsibility for handling incidents of Internet misuse will be taken by the Designated Safeguarding Lead and/or Deputy Designated Safeguarding Lead.
- Any complaint about staff misuse of digital technology must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- There may be occasions when discussions will be held with the police support services to establish procedures for handling potentially illegal issues.
- Where possible the school will liaise with local organisations to establish a common approach to e-safety.

11. Communicating the E-Safety Policy

Introducing the e-safety guidelines to pupils

E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year and then as appropriate.
Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

All staff will be given the School E-Safety Policy and the importance of it explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

If a colleague at the school believes they will have any difficulty complying with any of the requirements in these guidelines for whatever reason (for example, where they are related to a pupil), they should discuss the matter with the Headteacher. Failure to do so will be regarded as a serious matter.

Parental support

Parents' attention will be drawn to the School e-safety guidelines in newsletters, the school brochure, on the school web site and during the e-safety events.
Parents will be asked to read through the *ICT Acceptable Usage Agreement for Pupils* with their child and co-sign it on an annual basis.