Spalding Monkshouse Primary School

E-SAFETY POLICY

Review Date: October 2018

E-safety Coordinators	**Mr C Price/Miss E Dobbs**
Designated Safeguarding Officer	**Mrs S Wickham**
Designated Governor	**Mr S Lilley/Mr A Main**

United Nations Convention on the Right of the Child Article 17
You have the right to get information that is important to your well -being, from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. We understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Some of the potential dangers of using technology may include:

- 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 young person.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught
to manage them effectively.

Scope

This policy applies to all pupils, all staff, all Governors and all volunteers.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, cameras etc); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Aims

To ensure that all pupils:

- Will use the internet and other digital technologies to support, extend and enhance their learning
- Will be given clear objectives for internet use
- Will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world and the need to avoid undesirable material
- Will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working
- Will use existing, and up and coming technologies safely

Teaching and Learning

Why is Internet use important?

We use the internet for a number of reasons:

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own personal safety and security whilst online.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national
- developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.
- Exchange of curriculum and administration data with Local Authority and DfE

Infrastructure

The school will be responsible for ensuring that the school network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure effectively.

- School ICT systems are managed by ARK who ensure that the school meets the E-safety technical requirements in discussion with ICT coordinators.
- Regular reviews of the E-safety and security of the systems are conducted.
- Servers, wireless systems and cabling are securely located and physical access is restricted
- All staff have secure, independent login details of user name and password. Administration is managed by ARK.
- Users are responsible for the security of these. Any suspicion or evidence that there has been a breach of security must be reported immediately to the ICT coordinators.
- The school maintains and supports the managed filtering service provided by ARK.
- Requests from staff for sites to be added/removed from the filtered list will be considered by the E-safety coordinator.
- E-safety incidents should be logged on the appropriate forms (in PPA room) and handed to an E-safety coordinator (Callum Price/Emma Dobbs).
- Reference should be made to the photograph policy for use of images in school.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. Ensure these are backed up on the school system in the appropriate folders on a weekly basis.

Students / pupils:

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through letters, school website and information about national and local e-safety campaigns.

Parents and carers will be responsible for:

Endorsing (by signature) the Student / Pupil Acceptable Use Policy

Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.

- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely
Pupils will be taught about E-safety throughout the year and on designated E-safety week.

.

E-mail
- Pupils and staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff if they receive inappropriate E-mail communications
- Pupils will only use e-mail for approved activities

Internet Access
- Staff will read and sign the Acceptable Use Policy before using any school ICT resource
- Parents will read and sign an Acceptable Use Agreement before their children will be given access to internet resources. KS2 children also sign an agreement.
- Pupils will be taught to use the internet responsibly and report any inappropriate content to a responsible adult.

Mobile phones
Pupils are not allowed to have mobile phones in school with them. Any brought have to be handed to the office on arrival and picked up at the end of the day.

School Website
The school website is hosted on a server in the UK. The safety of children and other users who appear or are referred to on the published site is of paramount importance.

The school will ensure that no pupil's images will appear on the website without parental consent and, that they cannot be contacted either via or as a result of using, the school website. Any images of children will not be labelled with their names.

Adults' names will be published as their title and last name e.g. Mr Smith. Children's names will be published as their first name only e.g. Jacob, or if required, first name and year group e.g. Jacob Y4.

Permission will be obtained from parents or carers before publishing the work of any pupil. Only first names and year group will be used to identify the work.

Children will only be shown in photos where they are suitably dressed.

Personal details of children or staff such as home addresses, telephone numbers, personal e-mail addresses, etc, will not be released via the website.

Links to external websites will be checked thoroughly before inclusion on the school website. The sites will be checked for the suitability of their content for their intended audience.

All written work will be reviewed to ensure that it is in no way defamatory.

All written material will be checked for its suitability for its intended audience.

Adults have the right to refuse permission to publish their image on the site.

Parents have the right to refuse permission for their child's image to be published on the site.

Communication of the E-safety policy to pupils

- Pupils will read (or be read) and sign the age appropriate Acceptable Use Agreement before using these resources.
- E-safety rules will be posted in the ICT suite
- Pupils will be informed that internet use will be monitored.
- E-safety will be included in the curriculum and regularly revisited and a designated week will be included in the diary for specific focus
- Key E-safety messages will be given in assemblies

Communication of the E-safety policy to staff

Attention will be drawn to E-safety and acceptable use policies and they will be signed and discussed at least annually.
Staff will be informed that internet use will be monitored.

Communication of the E-safety policy to parents/carers

- The acceptable use policies will be available on the school website and requests can be made for hard copies.
- An E-safety booklet is available on the website or in hard copy
- Parents will be asked to sign a home-school agreement when their children join the school. This will include acceptable use policies relating to the internet, The school will communicate and publicise E-safety issues to parents through the newsletter and the website and will offer workshops to parents.

E-safety complaints

- Instances of pupil internet or Learning Platform misuse should be reported to a member of staff.
- Staff will be trained so they are able to deal with E-safety incidents. They must log incidents reported to them inform the E-safety coordinator
- Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher.
- Pupils and parents will be informed of the consequences of internet misuse

Roles and Responsibilities

Governing Body

The Governing Body will:
- Appoint an E-safety governor who will ensure that E-safety is included as part of a regular review of child protection and health and safety policies
- Support the Headteacher and E-safety coordinator in establishing and implementing policies, systems and procedures in order to ensure that there is a safe learning environment at the school
- Ensure that appropriate funding is available for E-safety

The Headteacher and senior leaders will:
- Ensure the E-safety of the school community, though the day to day responsibility for E-safety will be delegated to the E-safety coordinators
- Be kept informed of any E-safety issues
- Be aware of procedures to follow in the case of an E-safety allegation being made against a member of staff (see end of policy)
- Provide time for the E-safety coordinators to conduct their role effectively
- Ensure the Governing Body is kept up to date

E-safety coordinator will:
- Take day to day responsibility for E-safety issues and have a leading role in establishing and reviewing the school's E-safety policies and documents
- Ensure staff are aware of procedures that need to be followed in the event of an E-safety incident taking place
- Provide training and advice for staff
- Liaise with Ark and E-safety governor
- Receive and action reports on any E-safety incidents (liaising with DSO) and create a log of events to inform future actions
- Report to SLT
- Provide workshops/information for parents

Ark and their technical support staff will:
- Ensure that the school's infrastructure is secure and not open to misuse or malicious attack
- Ensure that users may only access the networks and devices through a properly enforced password protection policy
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- Have an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the E-safety coordinator.
- Ensure that they keep up to date with E-safety technical information
- Ensure that filtering is updated on a regular basis

Teaching and Support Staff will:
- Have an up to date awareness of E-safety matters and of the current school E-safety practices and policies.
- Adhere to Acceptable use policies

- Take responsibility for the security of data.
- Transfer data using encryption and secure password protected devices, ensuring this is backed up on the school system in appropriate folders on a daily basis and a back-up report issued
- Develop an awareness of E-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include E-safety regularly in the curriculum.
- Ensure pupils understand and follow the school's E-safety and Acceptable Use policies
- Monitor ICT activity in school, extra curricular and extended school activities
- Report any E-safety issues they become aware of to the appropriate person
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Pupils will:
- Be responsible for using the school ICT systems in accordance with the
- Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, taking / use of images and on cyber-bullying
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school

Parents/carers
Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile deices in an appropriate way. Research shows that many parents/carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will take every opportunity to help parents understand these issues by sharing information about national and local E-safety campaigns through the newsletter and school website. Parents should:

- Read acceptable use policies and encourage their children to adhere to them.
- Read the school's E-safety booklet
- Adhere to acceptable use policies
- Discuss E-safety issues with their children, support the school in its E-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online

Reporting Incidents
Children should follow this procedure:-
- Stop using a site immediately
- Tell a member of staff as soon as possible

Adults in school should:

Stop children using any inappropriate sites immediately

- Record incident on E-Safety Log
- Note down any site's URL and name
- Report as soon as possible to the e- safety coordinator, who will email ARK and get the site banned using our filtering system

Responding to incidents of misuse

Illegal incidents
If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the flow chart attached to this policy.

Other incidents
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- More than one senior member of staff should be involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- The procedure should be conducted using a designated computer that will not be used by students and if necessary can be taken off site by the police should the need arise. The same computer should be used for the duration of the process.
- Relevant staff should have appropriate internet access to conduct the procedure, and sites and content visited closely monitored and recorded to provide further protection.
- The use of any site containing the alleged misuse and the nature of the content causing concern should be recorded. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. This may be printed, signed and attached to the form (except in cases of child sexual abuse).
- Once fully investigated the group should judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following;
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisations (as relevant)
- Police involvement and / or action

If the content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material

- Other criminal conduct, activity or material

Isolate the computer in question as best you can. Any changes to its state may hinder a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the school police and demonstrate that visits to these sites were carried out for child protection purposes.

School actions and sanctions
It is more likely that the school will need to deal with incidents that involve inappropriate rather illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be through normal behaviour / disciplinary procedures and could include:

Pupils:
- Referral to class teacher
- Referral to KS leader
- Referral to E-safety Coordinator(s)
- Referral to Headteacher
- Referral to the Police
- Referral to technical support staff for action re filtering / security etc.
- Informing parents / carers
- Removal of network / internet access rights
- Fixed Term Exclusion
- Permanent Exclusion

Staff:
- Referral to Line Manager
- Referral to Headteacher
- Referral to HR
- Referral to technical support staff for action re filtering etc.
- Warning
- Suspension
- Disciplinary action
- Referral to the Police
- Dismissal

Monitoring
The school will monitor the impact of the policy using:
- logs of reported incidents(reported to coordinator)
- surveys / questionnaires from
  - students / pupils
  - parents / carers
  - staff

Governors will be kept informed by IT Governor feedback and Headteachers report.

Signed_____Chair of Governors

Signed_____Headteacher

Date _____

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.

Appendix 2 - E-Safety Audit

This quick self-audit will help the Senior Management Team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those details within Appendix 1.

Date of latest update: September 2016	
The policy was agreed by Governors on:	
The policy is available for staff at: on the 'G' Drive and a paper copy in the school office.	
And for parents: In the school office or on the school website.	
The Designated Child Protection Coordinator is: Mrs S. Wickham	
The E-Safety Coordinators are: Callum Price and Emma Dobbs	
Has E-Safety training been provided for both students and staff?	Y
Do all staff sign an ICT Code of Conduct on appointment?	Y
Do parents sign and return an agreement that their child will comply with the School E-Safety Rules?	Y
Have school E-Safety Rules been set for students?	Y
Are these rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DCFS requirements for safe and secure access?	Y
Has an ICT security audit been initiated by SMT, possible using external expertise?	Y
Is personal data collected, stored and used according to the principles of the Date Protection Act?	Y

Appendix 3

Monkshouse Primary School

E-Safety Incident Log

Details of *ALL* E-Safety incidents will need to be recorded by the staff members/class teachers/e-Safety Coordinator. This incident log will be monitored termly. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons