Barmby Moor CE Primary School
E-Safety Policy

School Mission Statement

Our school nurtures the very best in each individual, providing a high standard of teaching and learning. Our Christian values encourage care for all, mutual respect, responsibility and strong partnerships between school, home and church.

Rationale

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. At Barmby Moor CE Primary School, we understand that we have a responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and 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.

Information and Communications Technology covers a wide range of resources including: web-based and mobile learning. It is also important to recognize 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 Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other 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.

Aims

- To provides opportunities within a range of curriculum areas to teach children about e-safety.
- To educate pupils on the dangers of technologies that they may encounter outside of school. This will be done both informally when opportunities arise and as part of the e-safety curriculum.
- To make pupils aware of the relevant legislation when using the internet such as data protection.
- To teach pupils about respecting other people's information, images, etc through discussion, modelling and activities.
- To make pupils aware of online bullying and know how to seek help if they are affected by these issues. Pupils will also be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. class teacher /e-safety coordinator – Mr Dale & head-teacher Mrs Chadwick.
- To critically evaluate the materials they find and learn good searching skills through the ICT curriculum.

E-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in our school is Mr Dale. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as East Riding Safeguarding of Children Board and CEOP (Child Exploitation and Online Protection) and Childnet, as well as through reading current Ofsted reports relating to e-safety.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour (including the anti-bullying) policies.

Role of the E-safety Co-ordinator

1) To provide leadership, expertise, advice and assistance for members of staff.
2) To develop and implement appropriate record keeping on any e-safety issues
3) To ensure that the policy for e-safety is regularly evaluated and updated, is known and understood by staff and provides continuity and development throughout the school.
4) To liaise with governors as appropriate, in particular the governor for e-safety – Mr. Shaun Williamson
5) To monitor and assess standards and quality of teaching and learning using observations, standardized data, monitoring of work and lessons. From this to know strengths and weaknesses of implementation of e-safety throughout the school.
6) To identify and inform the Head teacher/E-safety co-ordinator of resources and training needs.
7) To create an annual development plan which will inform the school's improvement plan.
8) To be aware of, and identify, INSET needs - making use of expertise available inside the school, liaise with the LEA e-safety Officer and through organizations such as The Child Exploitation and Online Protection (CEOP).
9) To be conversant with current thinking and developments in understanding and delivering e-safety messages. The school's e-Safety coordinator ensures the Head, all staff and Governors are updated as necessary.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues.
- New staff receive information on the school's acceptable use and e-safety policies as part of their induction.
- All staff, whether based permanently at our school or visiting staff (e.g. sports coaches and peripatetic music staff) have read and signed our acceptable use and e-safety policy kept in the Safeguarding Policies Folder kept in the Staff Room.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Managing the school E-Safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety information will be available via the school website

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are regularly reminded of the need for password security on laptops as well and pen sticks and external hard drives. .

- All users read and agree to abide by an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety policy.
- Users are provided with an individual network username.
- Pupils are not allowed to deliberately access materials or files on the school network, of their peers, teachers or others, unless these have been made publicly available.
- If you think your password may have been compromised or someone else has become aware of your password you should change your password immediately and report this to the e-safety co-ordinator.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared. Individual staff users must also make sure that workstations are not left unattended and are locked.

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Infrastructure

- School internet access is controlled through the filtering service.
- Barmby Moor CE Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator if appropriate, he will then complete the log and carry out an investigation.
- It is the responsibility of the school to ensure that anti-virus protection is installed and kept up-to-date on all school machines. If there are any issues related to viruses or anti-virus software.

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission of the head teacher or ICT co-ordinator unless from an education website.

Special Educational Needs, Inclusion and Equal Opportunities

- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules. However, staff are aware that some pupils may require additional teaching including (visual) reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
- Where a pupil has poor social understanding or Special Educational Needs, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.
- Some students may find it difficult to explain or describe events and may need to replay (distasteful) scenarios in order to aid their recall. Some students may not be aware of the consequences of their actions or that they may require or should ask for help at all. Sensitive and context-dependant handling of such issues by staff is required.

Pupils

- At present, Barmby Moor Primary School endeavours to deny access to social networking sites to pupils within school and to deter them from accessing adult social networking sites out of school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are reminded that posting material which may be construed as offensive relating to the school, pupils or staff, on any internet site is considered by the school as cyber bullying and appropriate action will be taken.
- Any video/images taken that show the school site and/or students in school uniform are considered to be inappropriate for uploading to the internet unless the permission of the Head Teacher has first been given.
- Our pupils are asked to report any incidents of bullying to the school via their class teacher.

Staff

- Staff are advised to employ caution when posting any material on the internet relating to themselves and their activities. The **golden rule** is to ensure that there would be no embarrassment or other consequences if something posted were read by the Head Teacher or pupils of the school.
- Staff are advised that, once posted on the internet, personal material may be publicly available for many years. All staff, and especially new staff, are therefore advised to check that no material about themselves can be found on the internet that would not meet the **golden rule**.
- (Remember that sometimes your image may be 'tagged' by other friends and acquaintances). Advice on this matter can be sought from the e-safety co-ordinator who will liaise with the Head Teacher if required.
- Staff are advised to use social networking and other similar sites (eg YouTube/Flickr/Facebook/Twitter) only with caution and to use the security features to ensure maximum privacy settings. Under no circumstances are staff allowed to accept a student as a 'friend' on any personal social networking site unless that student is a close relative (ie son/daughter/brother/sister etc). When posting, even with maximum privacy settings, staff are advised to remember the **golden rule**. Staff should seek the advice of the e-safety co-ordinator.
- Staff are advised only to create blogs, wikis for educational purposes using the school website where appropriate.
- Any video/images taken that show the school site and/or students in school uniform are considered to be inappropriate for uploading to the internet (whether for educational purposes or not) unless the permission of the Head Teacher has first been given.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Pupils are not allowed to bring personal mobile devices/phones to school but in circumstances where this is unavoidable the mobile device will be stored in the school office and collected by a parent/carer at the end of the school day.
- This technology may be used, on occasion for educational purposes. The device user, in this instance, must always ask the prior permission of the bill payer and Head teacher.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission of the subject(s) must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (cameras and digital video cameras)

The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission of the subject(s) must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as laptops and video cameras for offsite visits and trips, only these devices should be used.
- The school memory card should be used in personal cameras

Managing Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including: direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level four or above, pupils must have experienced sending and receiving emails.

- The school, via the ICT co-ordinator, should give all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. An additional staff email address is available via the ICT co-ordinator upon request if staff wish to have an exclusive email address for use by pupils.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette ('netiquette'). This is particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in e-mail communication, never arranging to meet anyone without specific permission and virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail (do not delete the email as it will be needed as evidence). This should be reported to the class teacher who may decide to forward this for action to the e-safety co-ordinator or headteacher.
- Staff must inform the e-safety co-ordinator and head teacher if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work for Year 2.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided the camera has the school's memory card and is inserted on to the school's network.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips and other residential visits. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.
- Where possible, general shots of classroom or group activities should be taken rather than close-up shots of individual pupils. Care should be taken to ensure that students are in suitable dress (particularly relevant for PE activities). Staff should also be mindful of including images of children from different ethnic backgrounds and with disabilities to promote the school as an inclusive community and to comply with the Disability Discrimination Act.

Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing pupils' images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use and store their child's work/photos in the following ways:

- on the school computer network
- on the school website
- on the internet uploaded to websites previously approved by the headteacher or e-safety co-ordinator
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
Parents/ carers may withdraw permission, in writing, at any time.

Pupils' full names will not be published alongside their image (i.e. either image and first name or full name with no image). E-mail and postal addresses of pupils will not be published.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- The e-safety co-ordinator has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Parental right to take photographs and videos

Parents are permitted to take photographs and videos at school events for their own personal use only (unless this is expressly prohibited – for example at school plays where there are third party copyright regulations which prohibit recordings). Recording and/or photographing other than for private use would require the consent of other parents whose children may be captured on film. Without this consent, the Data Protection Act 1988 would be breached.

Official School Photographs

From time to time the school will invite an official photographer into school to take photographs of individual children and house/form groups. The school will ensure that appropriate CRB checks have been made with the company concerned.

Misuse and Infringements

Complaints and Reports

Complaints and reports relating to e-safety should be made initially to the e-safety co-ordinator who will then liaise with other members of staff/students/parents as appropriate. The only exception to this is with incidents of cyber bullying when the class teacher is generally the first point of contact. The class teacher in this instance will liaise with the e-safety co-ordinator and head teacher. All incidents will be logged and appropriate action taken and recorded.

Sanctions

A variety of sanctions may be used according to the type and seriousness of the incident. These may include, but are not limited to:

- A ban from the school network for a fixed period
- Parents to be informed
- A verbal/written warning

Inappropriate material

- All users are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator if appropriate.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA.
- Users are made aware of sanctions relating to the misuse or misconduct of the school computer network as part of the acceptable use policy which they must signed up to.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety policy by contacting the e-safety co-ordinator to discuss e-safety issues.
- Parents/ carers are asked to read through the school acceptable use agreements that their child has been asked to sign up to.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information evenings, displays and posters
    - Website
    - Newsletter items

Writing and Review of the E-Safety Policy

Our e-Safety Policy has been written and edited by the E-safety co-ordinator and all staff.

Staff involvement in policy creation

- Staff have been involved in making/ reviewing the e-safety policy through information sessions.
- The policy has been approved by the School Governors.

Review Procedure

- There will be an on-going opportunity for staff to discuss with the e-safety co-ordinator any issue of e-safety that concerns them.
- This policy will be reviewed every 6 months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Signed…….. Date……..
Chair of the Governors

Signed…….. Date……..
Headteacher