Balby Central Primary School

Policy for e-safety

Date of Policy: January 2016
Approved by the Governing Body:
Review Date: January 2017

All pupils use computer facilities including Internet access as an essential part of learning. Teachers, pupils and their parents/carers are asked to sign to show that the e-safety Rules have been understood and agreed.

Writing and reviewing the e-safety policy

- Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.
- The e-safety Policy and its implementation will be reviewed annually.
- The e-safety Policy was revised on: January 2016
- It was approved by the Governors on:

Teaching and learning

Why Internet use is important

- 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. It is 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.
- Internet access is used to enrich and develop learning as it can play a vital role in promoting pupil achievement and raising attainment.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.

Internet use will enhance learning

- The school Internet access is designed specifically for pupil use and is filtered age appropriately. Only suitable content is accessible, which will extend and enhance learning.
- Internet access enriches and develops learning through a variety of mediums and resources.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives.
- Pupils will be educated in the effective use of Internet research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be encouraged to use on-line activities that will support learning and that are appropriate for the students' age and maturity.
- It provides access to world-wide educational resources to support learning.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- They will develop critical skills in selection and evaluation.
- Pupils will use age-appropriate tools to research Internet content.
- We will inform our pupils about current e-safety issues; teaching them 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.
- Staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Teaching, support staff (and Governors where relevant)
are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher for investigation
- all digital communications with pupils, parents or carers should be 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 (teachers to use recommended e-safety planning alongside the Rising Stars e-safety guidance to ensure that the children know how to use the internet, games and social media safely).
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child protection

Staff should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Training
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. 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 policy and Acceptable Use Agreements.
- The e-safety co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This e-safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The e-safety co-ordinator / Officer (or other nominated person) will provide advice , guidance and training to individuals as required.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Doncaster LA.
- Access by wireless devices is proactively managed and secured with a password encryption.
- User logins and passwords are in place and need to be inputted in order to access the schools network.
- Personal data that is taken off site will be encrypted.
- The ICT technician will review the system's capacity regularly.

Using the internet safely

- Instructions in responsible and safe use by children will precede Internet use.
- Children's access to the Internet will be by adult demonstration or directly supervised to specific online material.
- As part of the curriculum children will be made aware of the guidelines for acceptable use of the Internet and what is not acceptable.
- The school has a duty of care teach children e-safety for use of the Internet when not at school. Children will be taught the security risks of accessing certain types of content.
- Children will be taught of the dangers of giving out any-one's personal information via email, social network sites and online generally. They should be aware that they should never meet in person some-one that they have 'met' online without an adult with them.
- Children will be taught about e-safety using the S.M.A.R.T steps.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class email addresses may be used for external communication for educational benefits. Such as for projects between neighbouring schools.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

Published content and the school website

- The school websites will be used to celebrate pupils' work, promote the school and provide additional information about current events in school.
- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Staff posting content online will take overall editorial responsibility and ensure that content is accurate and appropriate.
- We will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Children's images must only be put on the website or Facebook page if permission was given from their parents/carer.
- Children are not allowed to edit the website but are encouraged to access it in their own time.

Publishing pupil's images and work

- The school websites will be used to celebrate pupils' work and promote the school.
- Photographs that include pupils will be selected carefully and only children with consent will be allowed online.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing (To work alongside with the Social networking policy 2015-16)

- 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.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- Pupils and staff will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community, including on social media sites.
- Concerns regarding students' use of social networking, social media and personal publishing sites will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staffs personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined. They will also be asked to sign the 'Acceptable ICT Use Agreement'.

Managing filtering

- The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- Mobile phones will not be used during lessons or formal school time by staff or pupils. The sending of abusive or inappropriate text messages is forbidden.
- Staff should use the school phone to contact parents or external agencies (school related).

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All parents must read and sign the 'Acceptable ICT Use Agreement' on behalf of their children, before they can use any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Access to the Internet will be by adult demonstration or by supervised access to specific, approved on-line materials and sites.

Assessing risks

- The school and DMBC 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 cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme to raise the awareness and importance of safe and responsible Internet use will be used at least once a term.
- Instruction in responsible and safe use precedes any lesson with Internet access.
- E-safety concerns will be addressed in ICT and PSHE lessons, covering both school and home use.

Staff and Governors the e-Safety policy

- All staff and governors will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff will be issued with a school login and asked to sign an 'Acceptable ICT Use Agreement'.

Enlisting parents' support

- Parents will be offered demonstrations and suggestions for safe home Internet use.
- They will also be given advice on filtering systems and educational and leisure activities that include responsible use of the Internet.
- In addition, parents will be provided with current information about online resources that may not promote e-safety or be suitable for children.

- All parents must read and sign the ‘Acceptable ICT Use Agreement’ on behalf of their children, before they can use any school ICT resource.

Failure to Comply

- Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff.