

SIR JOHN BARROW PRIMARY SCHOOL E-SAFETY POLICY

1 INTRODUCTION

1.1 This policy has been developed to ensure that all adults in **Sir John Barrow Primary School** are working together to safeguard and promote the welfare of children and young people.

1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the School community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4 The Headteacher, the Deputy Headteacher or SLT have the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 This policy complements and supports other relevant School and Local Authority policies.

1.6 The purpose of internet use in School is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the School's management information and business administration systems.

1.7 The internet is an essential element in 21st century life for education, business and social interaction and the School has a duty to provide children and young people with quality access as part of their learning experience.

2 ETHOS

2.1 It is the duty of the School to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the 'Help Children Achieve More' agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the School's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the School and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-Safe practices in School and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, School equipment or the School day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the School's Anti-Bullying and Behaviour Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the School's Safeguarding Policy.

3 ROLES AND RESPONSIBILITIES

3.1 The Headteacher of Sir John Barrow Primary School will ensure that:

- All staff should be included in E-Safety training which will be carried out in house and closely informed by this policy. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- All temporary staff and volunteers are made aware of the School's E-Learning/Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers will act as the first point of contact with regards to breaches in safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's E-safety Policy.
- Ensure that all staff and volunteers understand and are aware of the school's E- Safety Policy.
- Ensure that the School's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Ensure that files are regularly checked on the School's network.

3.2 The Governing Body of the School will ensure that:

- There is a member of the Governing Body who is designated to take the lead on E-Learning/Safety – Mrs Janet Heffernan (*nominated eSafety Governor*).
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures (see Cumbria Acceptable Use Policy)

4 TEACHING and LEARNING

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DCSF.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

4.7 Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5 MANAGING INTERNET ACCESS

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The School internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people (supplied by CLEO)

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. (see Rules for Responsible Use of Computers) Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. (see Rules for Responsible Use of Computers)

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to OneConnect (previously CLEO) via the ICT Subject Leader / SLT/ UVHS technical team. URL's can be recorded in the ICT book in the main office or on the spreadsheet on the server.

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

6 MANAGING E-MAIL

6.1 Personal e-mail or messaging between staff and pupils should not take place.

6.2 Pupils and staff may only use approved school-based e-mail accounts on the School system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole –class or group e-mail addresses should be used at KS1 and below.

6.3 Pupils must not reveal details of themselves or others in any email communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone. It is advised that children only share their first name in e-mails.

6.4 Access in School to external personal e-mail accounts may be blocked.

6.5 Pupils' E-mails should be authorised before sending to an external organisation just as a letter written on School headed note-paper would be. (Currently children do not have E-mail capability)

6.6 The forwarding of chain letters is not permitted.

6.7 Pupil's incoming e-mail will be monitored and attachments should not be opened unless the author is known.

7 MANAGING WEBSITE CONTENT

7.1 Editorial guidance will ensure that the School's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

7.3 The point of contact on the School website will be the School address, School e-mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the School's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused.

7.7 The names of pupils will not be used on the website, particularly in association with any photographs.

7.8 Work will only be used on the website with the permission of the pupil and their parents/carers.

7.9 The copyright of all material must be held by the School or be attributed to the owner where permission to reproduce has been obtained.

7.10 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

7.11 Pupils full names will not be written on the school blog, but permission will be sought by the school to include images/ first names where necessary.

8 SOCIAL NETWORKING AND CHAT ROOMS

8.1 Staff and pupils will not access social networking sites e.g. 'Facebook, 'Twitter' or 'MySpace' at school. (These are blocked by our internet service provider, CLEO)

8.2 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms via the KidSafe programme.

8.3 Pupils will not be allowed to access public or unregulated chat rooms.

8.4 Newsgroups will be blocked unless an educational need can be demonstrated.

8.5 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

9 MOBILE PHONES

9.1 Mobile phones will not be used during School hours. If children need to bring phones into school they are to be stored by their class teacher during the school day and returned to children at 3.15pm. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the School's Anti-Bullying and Behaviour Policies.

10 FILTERING

10.1 The School will work in partnership with parents/carers; the Local Authority, the DFE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 Regular checks by ICT Co-ordinator / SLT will ensure that the filtering methods selected are appropriate, effective and reasonable.

11 AUTHORISING INTERNET ACCESS

11.1 All staff must read and sign the Cumbria's Acceptable Use of ICT Policy before using any School ICT resources and any staff not directly employed by the school will be asked to read and sign Cumbria's Acceptable Use of ICT Policy before being allowed internet access from the School site.

11.2 The School will maintain a current record of all staff and pupils who are allowed access to the School's ICT systems.(from Log In accounts data)

11.3 The School will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.

11.4 Parents/carers will be asked to sign and return the School's form stating that they have read and understood and explained the School's 'Responsible use of Computers' document to their children and give permission for their child to access ICT resources.

11.5 Staff will supervise access to the internet from the School site for all pupils.

12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.2 Staff will not normally use personal photographic/video equipment in school. Staff may use school purchased photographic or video technology to capture school trips and appropriate curriculum activities. These photos will be uploaded and deleted from the device within 1 week. In the unusual circumstance of a staff member using personal equipment, the images/video will be uploaded and deleted on the same day.

12.3 Pupils must have permission from a member of staff before making a video or audio recording in School or on educational activities.

12.4 Webcam use will be appropriately supervised.

13 ASSESSING RISKS

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass School filtering systems and allow a new route to undesirable material and

communications.

13.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a School computer. Neither the School nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

13.3 Emerging technologies will be examined for educational use and Staff will identify, assess and minimise risks.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.5 The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14 INTRODUCING THE POLICY TO PUPILS

14.1 Rules for Responsible Computer use will be posted in all classrooms.

14.2 Responsible Internet use, covering both School and home use, will be included in the PSHE curriculum, through whole-school and team assemblies and via the KidSafe program.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

15 CONSULTING STAFF

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the School's 'Cumbria LA's Acceptable Use Policy' and will be provided with a copy of the E-Safety Policy and its importance explained.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.

- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- SLT members will supervise members of staff who operate the monitoring procedures.

16 MAINTAINING ICT SECURITY

16.1 Personal data sent over the network will be encrypted or otherwise secured.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails. Pupils do not have the right to install files.

16.3 UVHS IT Department will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

17 DEALING WITH COMPLAINTS

17.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the School's Safeguarding Policy and Procedures.

17.2 The School's designated person for E-safety (the Headteacher) will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately.

17.3 Pupils and parents/carers will be informed of the complaints procedure.

17.4 Parents/carers and pupils will work in partnership with the School staff to resolve any issues.

17.5 As with drugs issues, there may be occasions when the School must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system.

18 PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the School's E-Safety Policy which may be accessed on the school website.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.

18.3 In the case of an incident arising, advice on filtering systems and appropriate educational and leisure activities, including responsible use of the Internet, will be made available to parents/carers.

18.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

18.5 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

19 COMMUNITY USE

19.1 School ICT resources may be increasingly used as part of the extended school agenda.

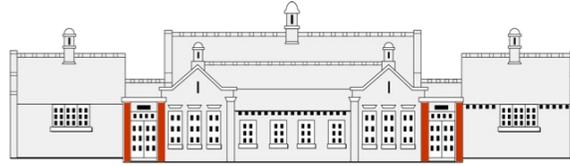
19.2 Adult users will sign the School's Rules for Responsible Use.

19.3 Parents/carers of children and young people under 16 years of age will be required to sign the Rules for Responsible Use on behalf of their child.

The Policy will be reviewed annually.

J Emms - ICT Subject Leader – November 2016

SIR JOHN BARROW PRIMARY SCHOOL



RULES FOR RESPONSIBLE USE OF COMPUTERS/TABLETS

These rules will help you stay safe and be fair to others.

I will not access other people's files

I will use the computers for school work and home work

I will not bring in pen drives from outside school unless I have been given permission

I will not use the internet without permission

I will only email people I know or my teacher has approved

The messages I send will be polite and responsible

I will not give my home address or telephone number or arrange to meet someone

I will instantly report unpleasant material or messages sent to me to a member of staff

I understand that the school may check my files and may monitor the internet sites I visit

I will use the iPads responsibly and for work related tasks