

Sherburn Primary School

Online Safety Policy And Acceptable Use Agreement

2015-2016

ONLINE SAFETY POLICY

Introduction:

ICT 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 children with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) 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
- ✓ Learning Platforms and Virtual Learning Environments
- ✓ Email and Instant Messaging
- ✓ Chat Rooms and Social Networking
- ✓ Music Downloading
- ✓ Gaming
- ✓ Mobile/Smart phones with text, video and/or web functionality
- ✓ Other mobile devices with web functionality (iPads, netbooks)

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. At Sherburn Primary School we understand that we have a responsibility to educate our pupils in online issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, tablets, mobiles phones, camera phones and portable media players, etc).

Roles and Responsibilities:

As online access and 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 online co-ordinators in our school are **S.Cornforth** (Headteacher) and **G.Jones** (Computing lead), all members of the school community have been made aware of who holds this post. The Online coordinator updates Senior Management and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice. The School has appointed a member of the Governing Body **D. Halliwell** to take lead responsibility for online safety.

Writing and reviewing the online policy:

This policy - supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils - is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying. Our online policy has been written by the school, building on the DCC e-Safety Policy and government guidance, and has been agreed by the Senior Management Team and staff and approved by the Governing Body. The online policy and its implementation will be reviewed annually.

Online skills development for staff:

- ✓ Our staff receive regular information and training on online issues through the co-ordinator at staff meetings.
- ✓ All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online and know what to do in the event of misuse of technology by any member of the school community.
- ✓ All staff are aware of how to report an incident and have been introduced to the incident log.
- ✓ All staff have agreed to and signed the school's Acceptable Use Agreement.
- ✓ New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- ✓ All staff are encouraged to incorporate online activities and awareness within their lessons. A progressive curriculum for online safety is ongoing and implemented across the school.

Online information for parents/carers:

- ✓ Parents/carers are asked to read through and sign the Acceptable Use Agreement alongside their child.

- ✓ Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- ✓ The school website and the Durham Learning Gateway contains useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page.
- ✓ The school will send out relevant online information through newsletters and parents meetings.

Community use of the Internet:

- ✓ External organisations using the school's ICT facilities must adhere to the online policy.

Teaching and Learning:

Internet use is part of the statutory curriculum and is a necessary tool for learning. In today's society, the Internet is a part of everyday life for education, business and social interaction. Sherburn Primary 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 safety and security. 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. Therefore, developing effective practice in using the Internet for teaching and learning is essential.

Internet use will enhance learning:

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- 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;
- exchange of curriculum and administration data with DCC and DfE;
- access to learning wherever and whenever convenient.
- The school will provide opportunities within a range of curriculum areas to teach online.

- Educating pupils on the dangers of technologies that may be encountered outside school is done when opportunities arise and as part of the online curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use, guiding the pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils will be taught how to evaluate Internet content:

The quality of information received via newspapers, television and Internet sites is variable and everyone needs to develop critical skills in selection and evaluation.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to use search engines appropriately for their age.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Internet Access

Information system security:

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.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Durham County Council.
- The school will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office www.ico.gov.uk advice is available from www.ico.gov.uk/for_organisations/sector_guides/education.aspx
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

E-mail:

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents.

- 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.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- 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.
- Staff should not use personal email accounts during school hours or for professional purposes.
- Sensitive data must be encrypted before e-mailing (e.g: medical, safeguarding, SEND)

Published content and the school website:

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. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils Images

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. 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.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on Sherburn Primary School's Website, particularly in association with photographs.
- Pupils work can only be published with their permission or the parents.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use:

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc. Parents/ carers will be asked to sign a form agreeing to this alongside AUP's, or when their child starts our school or through home visits for new Early Years children and at the first visit for transferring students. In the majority of cases parents will be asked not to take photographs on school premises to safeguard all of our children.

Social networking and personal publishing:

- The school will block 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. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of online bullying to both their parents and the school.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- School staff are advised **NOT** to add past or present children as 'friends' if they use these sites. (A child is anyone under the age of 18 years.)

Managing filtering:

- The school's broadband access will include filtering.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The school will have system in place to make changes to the filter, including deciding who is responsible for authorising changes – the Headteacher.
- The school will work with DCC to review filtering.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- The school will work with DCC and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, online Coordinator or Headteacher.
- The ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

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.
- The use of portable media such as memory sticks will be monitored closely as potential sources of computer virus and inappropriate material. In the event of these items being used they must be encrypted if content includes personal data related to staff or pupils in accordance with data protection laws.
- Pupils are **strongly advised NOT** to bring personal mobile devices/phones to school. Any phones that are brought to school will be given to the school secretary who will store them securely and keep them in the school office until the end of the day.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff **should not** use personal mobile phones during designated teaching sessions, for any reason (texting, checking, phoning etc).

Protecting personal data:

The school will collect personal information about you fairly and will let you know how the school and DCC will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or DCC. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and DCC.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving, or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Durham County Council and as defined by the Data Protection Act 1998. You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access:

Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's online rules. These online rules will also be displayed clearly in all networked rooms. As well as this, all staff will read and sign the School Acceptable Use Policy before using any school ICT resources. The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy. Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability. When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Password Security:

Adult users are provided with an individual network, email and Durham Learning Gateway login username and password, which they are encouraged to change periodically. Staff should only use their email address for work related purposes and not personal matters. Staff wishing to access work e-mails on mobile phones and personal tablets must ensure the devices are pin protected. All pupils from R - Y6 are provided with an individual network username and password. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. Staff members are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Assessing risks:

Sherburn Primary 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. Neither the school nor DCC can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the online policy is adequate and that its implementation is effective.

Handling online complaints:

Complaints of Internet misuse will be dealt with by the Head Teacher and reported to the online coordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online coordinator and recorded in the online incident logbook. 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.

Online bullying management:

- Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- There are clear procedures in place to support anyone in the school community affected by online bullying.
- All incidents of online bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of online bullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence (children are encouraged to screenshot and show to a trusted adult).
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to online bullying and the school's online ethos.
- Sanctions for those involved in cyberbullying may include:
 - The bully being asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
 - Internet access may be suspended at school for the user for a period of time.
 Other sanctions for pupils and staff may also be used in accordance to the school's Anti-bullying, Behaviour Policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Communications Policy

Introducing the online policy to pupils:

- Online rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.
- Online Safety sessions will be taught across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- An Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the online policy:

- All staff will be given the School online policy and its importance will be explained.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
 - Any information downloaded must be respectful of copyright, property rights and privacy.

- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

The Learning Platform

All staff will be trained and given advice on how to effectively use the Durham Learning Gateway. All children will be given training on how to effectively use the Durham Learning Gateway. Password access is required.

Children will be informed that the sending of messages through the Durham Learning Gateway is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user of the Durham Learning Gateway should such behaviour be repeated. Any misuse of the Durham Learning Gateway will be reported to the Headteacher.

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, staff and governor community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff or pupils leave the school their account or rights to specific school areas will be disabled.

Any concerns about content on the LP may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of SLT before reinstatement.

- A pupil's parent/carer may be informed.

Monitoring and Review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the online Coordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually.

Date implemented 29.02.16

Policy approved by Head Teacher: S. Cornforth Date: 2.02.16

Policy approved by Governing Body: R. Pye (Chair of Governors) Date: 22.02.16

The date for the next policy review is March 2016.