Shadsworth Junior School

E-Safety Policy

Approved by:	Jackie Gallagher	**Date:**	
Last reviewed on:	Spring 2018		
Next review due by:	Spring 2020		

Ethos:

At Shadsworth Junior School the issue of e-safety is part of our overall commitment to the safeguarding and wellbeing of all our pupils. As a school, we aim to help children to keep themselves safe, including encouraging pupils to adopt safe and responsible practices and to deal sensibly with risk when using the Internet. We work to create a learning environment where everyone feels valued, secure and motivated to learn.

Aims:

Our aim is to provide our pupils access to the range of teaching and learning opportunities provided by the Internet and the technologies we use in everyday life whilst minimising the risk of any harm.

- We aim to ensure that all children are educated about the benefits and risks of using technology.
- We aim to provide our pupils with safeguards and awareness to enable them to control their online experience in and out of school.

Objectives of this Policy

- Children and staff should be able to use the Internet and technologies identified within this policy to enhance their teaching and learning.
- Children and staff should be taught a set of safe and responsible behaviours in order to help keep themselves safe on the Internet.
- Children and staff should be taught principles of e-safety to help safeguard them both within and outside of school.
- Parents and carers should be informed of the potential dangers of the Internet and its associated technologies and they should be supported by the school to take measures to ensure safe usage by all.

Using new learning technologies effectively and safely

This policy deals specifically with the educational and curriculum element of online safety. Guidance and procedure relating to infrastructure, networking and appropriate use of technology by staff are contained in the ICT security policy. Our online safety Policy has been written by the school, building on the Blackburn with Darwen policy guidance. It has been agreed by the senior leadership team and approved by Governors. It will be reviewed annually by members of the online safety group.

Writing and reviewing the online safety policy

The online safety Policy relates to other policies including those for ICT security, anti-bullying and for child protection.

- The Computing subject leader (Mrs Amanda Gaines) is the online safety lead.
- The Headteacher (Mrs Jenny Hetherington) is the child protection co-ordinator.

- It was approved by the Governors on: Spring term 2018

Why the Internet and communication technology use is important

'Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age…' Ofsted 2013.

The safe use of technology is part of the statutory curriculum and the internet a necessary tool for staff and pupils.

Ofsted guidance for schools recommends that all schools:

- provide an age-related, comprehensive curriculum for online safety that enables pupils to become safe and responsible users of new technologies
- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Use pupils' and families' views more often to develop online safety strategies.

School and community involvement in online safety policy and practice

At Shadsworth Junior School we believe that by involving representatives from all the school community in evaluating, formulating and reviewing online safety policy and practice, our children and staff will be the safest they possibly can be.

Involving children in policy, practice and educating others

The school has a pupil online safety group. Part of their role will be to contribute to online safety policy and practice and inform parents and peers of online safety issues on a regular basis.

Membership of the adult online safety group

A Safeguarding group is being established and consists of:
The Head teacher, Deputy head teacher, online safety lead, computing curriculum lead, online safety governor, technical support, inclusion lead, a member of support staff and a parent.

The group will meet once a term and a wider consultation will be carried out through consultation of parents, governors, pupil and staff.

Leadership of online safety

Our online safety lead is the computing subject leader:

The responsibilities of the online safety lead alongside the online safety group are to:

- Ensure membership of the online safety group represents a range of stakeholders in the school community
- Maintain own knowledge of wider online safety and online safety leadership through training, seeking advice, and signing up to regular updates
- Carry out an online safety audit to inform the review process
- Regularly review the effectiveness of online safety policy and practice
- With the computing subject lead, ensure the computing curriculum is progressive and age appropriate and that there are opportunities across the wider curriculum including PSHE to reinforce online safety messages.
- Ensure all school staff receive online safety training annually and that a record of training is maintained

- Provide updates on online safety policy and practice to governors
- With the school's technical support, ensure that appropriate filtering and anti-virus software is in place
- Maintain reporting procedures for online safety incidents - This may be part of a wider reporting system, but should include access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyber-bullying disclosures. There should also be a record of how it was dealt with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.
- Provide or source online safety information via the school website and termly newsletters.
- Ensure that appropriate acceptable use agreements are signed by pupils and parents and that permission for use of images and video is sought from parents (and pupils when appropriate).
- Ensure that the educational potential and possible online safety issues are investigated before using new technology.
- Annually review the schools online safety strategy, policy and practice

Online safety Education and Training

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. Current guidance stipulates that it is not sufficient to keep pupils safe in school. It is our responsibility therefore, to ensure they have opportunities to learn how to stay safe and deal with the risks associated with the internet and communication technology in the world around them. Keeping our children safe involves educating all members of our school's community, including governors, parents and all staff working in school.

Educating pupils

Our online safety curriculum

At Shadsworth Junior School we ensure that children have access to a progressive online safety curriculum across all year groups.

The National Curriculum 2014 for Computing stipulates that pupils:

- In key stage 1 are taught to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- In key stage 2 are taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Shadsworth Junior School we use a number of approaches to ensure our pupils are confident and safe users of technology in and out of school. To ensure pupils have access to an age-appropriate online safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote online safety through teaching pupils how to stay safe, how to protect themselves from harm, we:

- Introduce age appropriate school and classroom rules each year and reinforce them regularly
- Use progressive statements within the Computing curriculum scheme of work, to ensure that areas of online safety relating to communication, information online, creating and presenting ideas, and Computer Science are covered regularly. These are planned into either computing, PSHE or the general curriculum as appropriate. The Computing scheme can be found in staff shared/ learning challenge folder.
- Deliver online safety messages in assembly in response to need, to reinforce national initiatives and agendas such as Safer Internet Day and anti-bullying week.
- Before using a new device or online resource, pupils are taught how to use it safely and appropriately. This is reinforced regularly.

- Teach pupils to tell a trusted adult should they be worried of upset by anything they encounter online or when using communication technology. (All staff are made aware of what to do should if a pupil confide in them.)

The need to keep login details and other personal information private will be reinforced regularly when using the schools network and any other methods of communication agreed by the head teacher.

Pupils will be taught how to evaluate Internet content appropriate to their age.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Pupils will be taught about the dangers of radicalisation and extremism at an appropriate level for their age and staff are made aware of how to identify pupils at risk of being drawn into terrorism and how to challenge extremist ideas.

Educating parents

Children often seem more at home in the digital world than their parents. To ensure that children are the safest they possibly can be, we must educate parents about the risk of using the internet and communication technology for their children and the potential for their own use of technology to place themselves or their child at risk.

We ensure parents receive information and training by:

- Ensuring they are represented on our online safety group
- Providing links to information and resources for parents on our school website
- Providing regular updates to parents through newsletters
- Inviting parents to online safety assemblies
- Providing online safety information during events such as parents evenings
- Encouraging parents to act a role models when using technology

The school will share with parents and children, our belief that:

- The unsupervised use of social network spaces intended for adults outside school is inappropriate for pupils of primary age.
- PEGI and BBFC ratings are good indicators of how appropriate the levels of violence, sexual content, bad language and the portrayal of drug taking and criminal acts are.
- Family friendly filtering can help to keep children safe, however education and the opportunity to develop safe practice is essential for keeping children safe.
- Pupils who use the internet and other communication technology may be at risk of being groomed or radicalised. It is important that parents understand that secrecy is a possible factor in both of these.
- What pupils do online now, can affect their future life.
- If a child is happy to tell a parent or carer when they are worried, they are the safest they can possibly be; therefore we encourage parents to nurture a sense of trust between them and their child when talking about using technology.

There are some excellent online tools for reporting concerns, such as the Report Abuse button which can be found on the https://www.thinkuknow.co.uk/ site and Childline http://www.childline.org.uk , Both these website links are available on our school website. Children are also encouraged to report their concerns to a member of staff or trusted adult.

Educating staff and the wider school community

- All school staff have access to basic online safety training regularly
- The online safety lead and key members of the online safety group have access to a higher level of training, updates and information to ensure that have the skills and knowledge necessary to lead all areas of online safety.

Basic training includes

- Online safety issues for pupils
- Reporting procedures
- Guidance on appropriate use of communication technology by staff and pupils
- Guidance for staff on how to stay safe
- Expectations in terms of passwords and data security
- Expectations in terms of professional conduct including the use of social media
- Teaching pupils to minimise the screen if they see something that makes them feel uncomfortable.

Online safety training references and complements guidance in the Safer Working Practices document.

Keeping staff and pupils safe in school

All access to the internet is filtered by Light Speed. For further details on networking and filtering and how access to inappropriate sites can be monitored refer to the ICT Security Policy.

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 online safety Lead who will inform the LA where appropriate so that they can take appropriate action.

All users will be taught how to care for devices in terms of health and safety. This includes avoiding placing food or liquids near to electrical devices, carrying equipment and rules around charging and electrical sockets.

Sanctions for inappropriate use of the internet and communication technology follow sanctions set down in the behaviour policy.

At Shadsworth Junior School staff do not use their own personal devices/accounts to contact parents and pupils. To protect staff and pupils, the school provides a mobile phone for contacting parents when on trips and visits and school email addresses. Cameras are provided for recording school related activities. Images of children should not be stored on personal devices.

Acceptable use agreements

A home school agreement concerning access to the internet and communication technology will be signed by pupils and parents in the Shadsworth Junior School Welcome Pack.

- Class rules agreement
- Acceptable use agreement for school staff (see the ICT Security Policy)

Passwords security

Pupils are encouraged to keep their password private. Parents are encouraged to ask children to logon to their accounts and show them what they have been doing rather than ask children to share their passwords.

- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Children will be taught to minimise the screen should they encounter anything that makes them feel uncomfortable.
- Pupils may only use approved digital methods of communication on the school system.
- Pupils will be taught about the report abuse button (this can be found on many websites including our school website)
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Webcams will not be used during communication unless expressly agreed by the Headteacher.

Reporting online safety concerns

Children are encouraged to report their concerns via a member of staff. We also encourage the children to use national resources such as Childline and CEOP.

- A record of online safety incidents is kept in the behaviour record file.
- The nature of the incident and action taken are recorded with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.. This includes access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures.

Published content - This will also be referenced in the in the ICT Security Policy

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication 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 will use their school email accounts. (Personal accounts must not be used to communicate information)
- Staff are never to give personal email addresses to pupils
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (This may be through education and guidance, as directly reading everything is impractical)
- Where pupils publish work, there will be systems in place to check the content and pupils will be given clear guidelines about what can be published.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere, particularly in association with photographs..
- Written permission from parents or carers will be obtained before photographs or video of pupils are published.
- Where pupil's work is published the school will ensure that the child's identity is protected.
- Where school events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip

Parents using still or video cameras at school

- The school do not allow parents to video or take photographs during school performances or assemblies.

Managing Social networking Sites

- At present, the school endeavours to deny access to unmonitored social networking sites such as Facebook to pupils within school.
- There should be no communication between staff and pupils/parents through social networking sites such as Facebook.
- 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).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Staff are strongly advised not to contact a pupil or parent/ carer using their personal device.
- Pupils are allowed to bring personal mobile devices/phones to school but such devices must be switched off and kept in the teacher's drawer.

- If such a device is heard or seen during the school day it will be confiscated and a responsible adult will be required to claim it from the headteacher. In such circumstances the headteacher will give a reminder about 'e' safety.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Protecting personal data

See the ICT Security Policy for guidance

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Responsible ICT Use Agreement' before using 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.
- Parents will be asked to sign and return a consent form for their children to access the internet.

Assessing risks

- The 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 Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety co-ordinator and to the LA where necessary.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher and where appropriate inform the LA.
- 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 on request.

For further information, please see the ICT Security Policy

Communications Policy

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where pupils may access the internet and discussed with the pupils at the start of each year. Where possible images and symbols will be used to help make them accessible to young children.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Introducing the policy to parents

Parents' attention will be drawn to the School online safety policy and practice:

- in newsletters,
- in the school brochure
- on the school website

Staff and the e-safety policy

- All staff will be given the School E-safety policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Please see the ICT Security Policy for further information

Annual Safety Audit

This quick self-audit will help the senior leadership team (SMT) assess whether the online safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Does the school have an online safety policy and ICT Security Policy and reflects current practice?	**Yes**
Date of latest update: **November 2016**	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is: Mrs Jenny Hetherington	
The online safety Coordinator is: Mrs Amanda Gaines	
Has annual online safety training been provided for all school staff?	
Have all governors received online safety training?	
Is there a named online safety governor?	
Do all staff sign an ICT Code of Conduct on appointment?	
Do parents sign and return an agreement that their child will comply with the School online safety Rules?	Shadsworth Junior School Welcome Pack
Have school online safety Rules been set for students?	Taught in lesson. Also available on our School website.
Are these Rules displayed in all rooms with computers?	Yes
Is the online safety curriculum flexible, relevant and does it engage pupils' interest?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	Yes
Has an ICT security audit been initiated by SLT, possibly using external expertise?	No
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes
Does the schools' ICT Security policy compliment the online safety policy	Yes