St. Stephen's Tockholes C.E. Primary School

Online Safety Policy

2018

St. Stephen's Tockholes C.E. Primary School Online Safety Policy:

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, ICT security, anti-bullying and for child protection.

- The IT co-ordinator is the online safety lead
- The headteacher is the child protection co-ordinator.
- The online safety Policy was revised by the Teaching and Learning Committee
- It was approved by the Governors: May 2016

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 a part of the statutory curriculum and the internet a necessary tool for staff and pupils.

Ofsted guidance for schools 2013 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 St. Stephen's Tockholes C.E. Primary 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 is developing pupil online safety group as part of the role of School Council . 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 safeguarding group
A Safeguarding group is being established and consists of: The Headteacher, deputy headteacher, 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 wider consultation is carried out through consultation of parents, governors, pupil and staff.

Leadership of online safety

Our online safety lead is the IT co-ordinator

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 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 cyberbullying 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 and training for parents
- 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 St. Stephen's Tockholes C.E. Primary School we ensure that children have access to a progressive online safety curriculum across all year groups.

Early Years Foundation Stage, Early Learning Goal

> Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

In order to safely select and use technology we believe that children in the Foundation Stage need to be taught an age appropriate online safety curriculum. When working towards this Early Learning Goal we will ensure our children use technology safely so that by the time they leave the Foundation Stage they are ready to access the key stage 1 curriculum

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.
- In key stage 3 understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.
- In key stage 4 understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns.

At St. Stephen's Tockholes C.E. Primary School we use a number of approaches to ensure our pupils are confident and safe users of technology in and out of school. An overview of the safeguarding curriculum including online safety can be found in the Safeguarding group folder.

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, 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 on the curriculum in the subject area in staff shared. This scheme also defines the knowledge pupils should have acquired pre key stage 1
- 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 using communication technology. (All staff are made aware of what to do should if a pupil confides in them.)

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

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.

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 .

Children are also encouraged to report their concerns via a member of staff or trusted adult.

Educating staff and the wider school community

- We ensure that all new staff receive online safety training as part of their induction
- 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.

The school internet access is designed expressly for pupil use and includes appropriate filtering.

Sanctions for inappropriate use of the internet and communication technology follow sanctions set down in the behaviour policy. A record of any misuse kept by the Assistant Headteacher.

At St. Stephen's Tockholes C.E. Primary 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 at appendix …

- 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 click on Hector should they encounter anything that makes them feel uncomfortable.
- Pupils may only use approved digital methods of communication on the school system. E.g. communication tools in the Learning platform.
- Pupils in key stage 2 upwards 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

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.

Detail below systems for reporting online safety concerns. This should build on any systems for behaviour and safeguarding already in school. It should include:

- *A record of online safety incidents is kept in the Online safety file in the head teachers office*
- *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.
- 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. (In the Foundation Stage this may not be practical when capturing a child in the process of learning, however should be modelled as often as possible.)
- 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. (some schools may wish to use first names, where there is no photograph, but staff should be aware of the risks associated with this and take appropriate precautions)
- 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

- In line with the Information Commissioner's Office, the school allows parents to record video and images during performances for personal use only. We advise parents of this before each event.

Guidance for taking photographs and video during school performances and assemblies.

Information Commissioner's Office
http://www.ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_application/TAKING_PHOTOS_V3.ashx

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered and shared with staff before they are used in school.

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 online safety policy

- All staff will be given the School online 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