



ST JUST PRIMARY SCHOOL

POLICY for 'online' safety and Acceptable Use.



E-Safety and 'online' Responsibility: A Bowman

E-Safety and 'online' Governor: R. Newman

Date policy adopted: July 2017 (annual review or earlier to reflect changes in statutory responsibility)

Introduction

National guidance suggests that it is essential for schools to take a leading role in online safety.

Becta in its "Safeguarding Children in a Digital World" suggested:

"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for online safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

Development / Monitoring / Review of this Policy

This policy has been developed by Online Safety Coordinator –A Bowman.

It takes into account discussions/consultations with:

- Headteacher
- Teachers
- Support Staff
- ICT Technical staff
- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council

- INSET Day
- Governors meeting / sub committee meeting
- Parents evening
- School website / newsletters

The implementation of this Online safety policy will be monitored at regular intervals. The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online safety or incidents that have taken place.

Should serious e-safety incidents take place, the following external agencies should be informed: LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of:
pupils parent/carers, staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator A Bowman
- regular monitoring of Online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator A Bowman
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.
- The Headteacher and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see Whistleblowing Policy.)

Online Safety Coordinator: A Bowman

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for all staff
- liaises with other partnership schools / Local Authority
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Headteacher / Senior Leadership Team

ICT Technician: ICT 4

Under the authority of the Headteacher, the ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the LA is informed of issues relating to the filtering applied • the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he / she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator / Headteacher / Senior Leader for investigation / action / sanction

- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problem to the Online Safety Coordinator / Headteacher / Senior Leader for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and rules established for acceptable use
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- they uphold the principles of the **Staff Online Safety Charter (appendix 1)**

Child Protection Co-ordinator

Mrs J Larter and A Bowman are trained in online safety issues and , along with all adults in school, are aware of the potential for serious child protection issues arising from:

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

Pupils:

- are responsible for using the school ICT systems in accordance with the Acceptable Use Policy and the **Pupil Online Safety Charter (appendix 2)** created by pupils on a yearly basis.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' seminars, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the **Parent's Online Safety Charter (appendix 3)**.

Education – pupils

Online Safety education will be provided in the following ways:

- In accordance with the 2014 National Curriculum requirements, planned online safety teaching will be provided as part of Computing / PHSE / other curriculum areas (as relevant) and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of school computers / laptops / ipads / internet will be devised annually through discussion with pupils. These will be posted in classrooms and displayed on the Online Safety display board. Further guidance will be posted on ipad log-in screens.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Although, it is recognised many parents and carers have only a limited understanding of online safety risks and issues, they undoubtedly play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences.

With this in mind, the school will therefore seek to provide information and awareness to parents and carers through:

- Letters and newsletters
- Parent workshops and information sessions and literature
- Reference to relevant online guidance provided by the school website or in paper format by the school office

Education & Training – Staff

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

- Formal online safety training will be made available to staff
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Coordinator will receive regular updates through attendance at ICA meetings and training events / LA courses / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / online safety / health and safety / child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure /network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames.
- The “administrator” passwords for the school ICT system, used by the ICT Technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by ICT4
- The school has provided enhanced user-level filtering through the use of the ICT4 filtering programme.

- In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to ICT4.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician, Headteacher and A Bowman. • School ICT technical staff, the Headteacher and A Bowman (pupils only) regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person). Staff would consult A Bowman and the Headteacher. The issue would be reported in the incident log and dealt with accordingly.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The Staff Charter includes guidelines on the provision of temporary access of “guests” (eg students, visitors) onto the school system.
- The Staff Charter includes the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- The Staff Charter includes guidelines on allowing staff to / forbidding staff from installing programmes on school workstations / portable devices.
- The Staff Charter includes guidelines regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Online safety should be a continuing focus in all areas of the curriculum and staff should reinforce online safety messages, wherever possible, in the use of Computing across the curriculum.

- Where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use by making use of the VLE or through bookmarks. Processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit, thus encouraging responsible use.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician can temporarily remove those sites from the filtered list for the period of study. Any request should also be

brought to the attention of the Headteacher and Online safety co-ordinator (A Bowman) with clear reasons provided.

- Pupils should be taught in all lessons to be critically aware of the materials /content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

When using images and video, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow The Staff Charter guidelines concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, under no circumstances should the personal equipment of staff be used for such purposes.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school's home school agreement (which seeks parental consent) on the use of images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or the school's social network accounts. An updated list will be kept by A Bowman Online Safety co-ordinator, the Headteacher and the school office. This list will also be made available to all staff.

Communication technologies

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Headteacher or A Bowman – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place

on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications. • Whole class or group email addresses will be used at Foundation Stage / KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use

- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Data protection

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the headteacher. Any data which is impractical to ensure is kept in school (eg Reports) will be kept secure, by use of encrypted memory sticks which are password protected.

Acceptable Use Policy

Use of the Internet is now an integral part of people's lives. In spite of this, it is important schools continue to be aware of issues and problems and to continue to educate our children accordingly. It is important staff, pupils and parents understand the moral and ethical issues surrounding access to the Internet before allowing access.

There are a number of options available that restrict access to the Internet, but it must be understood that no system, other than a ban on using the Internet, can ensure users do not access material that is deemed inappropriate. Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political material is beyond many filtering programs. There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyber-bullying and identity theft which cannot be controlled by filtering systems. For these reasons, treating the use of the Internet as an issue that involves pupils, staff and parents has to be the most sensible approach.

In response to this, the most appropriate course of action is to develop a school policy on use of the Internet together with a home/school agreement.

St Just Primary School has an Acceptable Use Policy, together with rules for safe internet use. These rules are a joint agreement between staff and pupils as part of our Online Safety curriculum. The policy works in line with our Home School Agreement and is available to parents on request and electronically via our website.

Today millions of people use the Internet and e-mail on a daily basis. In recent years, use of the Internet has continued to increase, particularly with the introduction of mobile devices. This is not only for

business and personal use, but also for educational purposes. A wealth of educational resources is now available on the Internet and via mobile devices; and this continues to grow. At St Just Primary School, we believe that our pupils should have opportunity to use these emerging and changing technologies to support their learning and to equip themselves with the skills that will be required for lifelong learning.

Resources found on the Internet, are unlike those found in more traditional media. Historically, resources such as books, videos and other resources could be carefully selected for the learning process. The Internet, by its open and dynamic nature, may lead pupils to material over which the teacher has had no previous viewing and has therefore been unable to judge its suitability for classroom use. Although the school will endeavour to point pupils to relevant curriculum sites or to previously researched sites that have been identified as being relevant to the area of study, we also accept our responsibility in educating our pupils about responsible, respectful and safe use of the Internet.

Research using electronic methods is now fundamental to preparing pupils for citizenship and future employment possibilities. The school will ensure that opportunities for both integrating the use of the Internet into the curriculum and teaching pupils about online safety will be planned and that staff will guide pupils in line with Government guidelines.

The school recognises that training the staff in preparation for using the Internet and indeed any mobile technology in a safe manner is vital. The school will use a variety of agencies to train the staff in integrating new technologies into the curriculum. Staff will be given regular opportunities to discuss issues surrounding the use of the Internet and e safety and develop appropriate teaching strategies. In addition, relevant governmental guidelines will be made available to all staff as a point of reference.

The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate Internet material or receiving inappropriate e-mail. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the Online Safety Co-ordinator. The Co-ordinator will then ask the ICT Technician to inform the ISP of the address of the offending web site. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind pupils of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access inappropriate materials. Therefore, the school reserves the right to access the work area of any user to view files held in that area.

All pupils across the school have access to the Internet and are able to use the technology available. It is anticipated that access to younger pupils will be more directed, with autonomous use being available to older pupils. Where pupils are given freedom to search the Internet for information, they should be given clear learning objectives by their teacher. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, Online safety co-ordinator or the Head. Any incidents will be reported and logged by the Online safety co-ordinator.

Pupils will be taught to use e-mail, the Internet and mobile technology responsibly to reduce the risk to themselves and others. After being agreed by staff and pupils at the beginning of each year, rules for Internet access and the use of all technologies within school will be posted in each classroom and around the school. E safety will form an integral part of Computing lessons but will also be covered in regular assemblies and as part of our PSHE and SMSC programmes of study.

The school believes that access to the Internet and mobile devices will enable pupils to explore resources available from libraries, other schools, LAs and commercial content providers in a way that will enhance the learning process in ways impossible by other means. E-mail will allow communication to be made with other individuals and organisations, regardless of time and distance.

The school believes that access to this technology brings benefits to the learning processes that outweigh the possible risks that might be encountered.

Older children will be encouraged to accept some responsibility for their use of the Internet according to the Pupil Online Safety Charter.

The final responsibility for use of the Internet and online safety lies with the parents and guardians of our pupils. Therefore, the school asks parents to sign our Parent Online Safety Charter. In doing so, parents are giving their permission for their children to be educated in accordance with school policies. Parents will also be provided with support and guidance in maintaining their children's safety away from school, through regular events in school and through documentation provided on our website and through literature sent home.

This policy will be reviewed on a regular basis in line with the Online Safety Policy and any technological advances and developments.

Appendix 1 Pupil Online Safety Charter

Appendix 2 Staff Online Safety Charter

Appendix 3 Parent Online Safety Charter

Letter to parents

Dear Parents,

Responsible Use of the Internet

I ask that you read this letter and the attached policy and then sign and return the slip to school.

Millions of people today use the Internet and e-mail as part of their daily lives. At St Just, we recognise this, and believe our pupils should have the opportunity to learn about and use these emerging and changing technologies. This will not only help to support their learning across the curriculum but also equip the children with the skills they will require for life-long learning.

In order to develop their learning, our children have regular access to computers, laptops, mobile devices and to the Internet throughout the school. We are fully aware of the concerns and issues surrounding safe Internet use and have a clear policy in place for dealing with this, a copy of which is attached to this letter. Our Internet provider is filtered and any computer use is monitored by staff. E-safety rules are agreed by staff and pupils the start of each year. These are displayed throughout the school and are available to view on our website. Children in KS2 also have a safe computer use contract which they are asked to sign.

Should you have any further concerns or wish to discuss any aspect of Internet use, please do not hesitate to contact me at the school.

Yours sincerely,

J Larter
Computing / Online safety co-ordinator

PLEASE COMPLETE AND RETURN THE FOLLOWING SECTION

I have read and accept the Acceptable Use Policy for pupils.

I give my permission for my son/ daughter to use the Internet as part of their learning at St Just Primary School.

I understand that suitable guidance and supervision will be provided during access to the Internet.

Signed _____ Date _____

Name of son/daughter _____ Class _____