Shelton Junior School

Together, we learn, trust & succeed.

eSafety Policy

Headteacher Approval	Governor Approval	Shelton Junior School *eSafety Policy*
Name: Mr Jon Bacon **Date:** 28/11/2019	**Name:** Ms K Phillips **Date:** 28/11/2019	Last Reviewed: Nov 2019 Review date: Nov 2020

Policy review dates and changes

Date	By whom	Summary of changes made

Contents

Introduction

This policy enables Shelton Junior School to carry out our functions with a view to safeguarding and promoting the welfare of children under sections 175 and 157 of the Education Act (2002). The policy is in line with the following legislation and guidance:

- Working Together to safeguard Children (2018)
- Keeping children safe in education (2018)
- ‘What to do if you think a child is being abused’ (2015)
- Information Sharing (2015)
- Derby and Derbyshire Safeguarding Children Procedures (2018)
- Children Act (1989)
- Children Act (2004)
- Dealing with Allegations of Abuse against Teachers and other Staff (2017)
- Protection of Freedoms Act (2012)
- Data Protection Act (2018)

Please refer to Shelton Junior School’s safeguarding policy which is written in line with DCSB Safeguarding procedure.

Rationale

The Purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Shelton Junior School, with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Shelton Junior School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies, and to monitor their own standards and practice.
- Set clear expectations of behaviour relevant to responsible use of the Internet for educational and personal use.
- Have clear structures to deal with online abuse, such as cyber-bullying, which are cross-referenced with other school policies.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones
- Internet communications: e-mail and instant messaging
- Webcams and videoconferencing

Wireless games consoles

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

The main risks for our school community can be summarised as follows:

Content:

- Exposure to inappropriate content
- Ignoring age ratings in games (exposure to violence)
- Lifestyle websites (e.g. pro-anorexia, self-harm, suicide sites)
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact:

- Grooming
- Cyber-bullying in all forms
- Identify theft (including hacking Facebook profiles) and sharing passwords
- Radicalization

Conduct:

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online – Internet or gaming)
- Sexting (sending and receiving of personally intimate images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film

Ofsted, Inspecting E-Safety in Schools, 2013

According to The Prevent Duty (2015), there is also a need for schools to ensure that children are safe from terrorist or extremist material when accessing the Internet in schools. Schools should ensure that suitable filtering is in place…As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activities of extremist and terrorist groups.

Roles and responsibilities

- The e-safety coordinator should maintain the E-Safety Policy, manage esafety training and keep abreast of local and national e-safety awareness campaigns.
- The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.

- The Local Authority will audit their filtering systems regularly to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- The school will include e-safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem. We use the SMART rules and the following e-safety programmes:
    - CyberQuoll - www.cyberquoll.com.au
    - Think U Know - www.thinkyouknow.co.uk
    - Childnet - www.childnet.com
    - Childline
    - CBBC
- All staff must read and sign the Acceptable Use Policy
- Parents should sign the Parent Internet agreement at the front of their child's home-school diary at the beginning of each academic year
- Pupils should read and sign the Pupil Internet agreement at the front of their home-school diary at the beginning of every academic year
- The e-safety policy will be made available to all staff, Governors, parents and visitors.

Teaching and Learning

Why is Internet use important?

Developing effective practice in Internet use for teaching and learning is essential. The purpose of Internet use in schools 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 use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Shelton Junior School has a duty to provide pupils with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Children will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity; pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the Internet. However, this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example, to close the page and report the incident immediately to the teacher. Any inappropriate content will then be reported to the Local Authority, as soon as possible after the incident. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Network/Server security

- Users must act reasonably.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders.
- Servers will be located securely and physical access restricted. Staff and pupil logins will be kept separate. Pupils will not have any access to the staff drive.
- The server operating system will be secured and kept up-to-date.
- Virus protection for the whole network will be installed and current.
- Access by wireless device must be pro-actively managed.
- Portable media should not be used at school without a virus check.

E-mails

- Pupils may only use their approved school e-mail addresses, whilst at school.
- Pupils must immediately tell a teacher if they receive an 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.
- If teachers are unsure about the content or attachments in any e-mails sent to them (e.g. possible virus e-mails), they should speak to the E-Safety Coordinator.

School Website

The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Headteacher and E-Safety/ICT Coordinator will take overall editorial responsibility and audit the website to ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications, including: respect for intellectual property rights and copyrighting.

Use of images:

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking, including Facebook and Twitter:

- Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.
- Our school uses ClassDojo to communicate with parents and carers. Teaching staff can post on these technologies
- All pupils have had to have parental permission from their parents/carers to have their photo posted on Twitter. Their name and photo will never be posted together
- Staff are not permitted to access their personal social media accounts using school equipment at any time during school hours
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

- The Local Authority has blocked/filtered access to social networking sites.
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations.
- Pupils will be advised never to give out personal details of any kind, which may identify them and/or their location. Examples would include real name, address, mobile or landline numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social networking space.
- They should consider how public their information is and consider using private areas.
- Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location, e.g. house number, street name or school.
- If we are particularly concerned about a child or staff member's use of social networking, or if we receive concerns from others, we reserve the right to search for and check their social networking accounts.

Filtering

The school will work with London Grid for Learning (the Internet Service Provider) to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the ESafety Coordinator.

Emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in schools is allowed.

Mobile phones

Mobile phones will not be used by staff or pupils during lessons or formal school time. In particular, photographs must not be taken on mobile phones.

School cameras/Staff iPads should be the only devices used for taking photographs at school. These photographs should be transferred to the school's Staff Drive as soon as possible and deleted from the device.

All mobile phones brought into school by pupils will be handed into the school office at registration and collected at the end of the school day. Only pupils who walk to or from school independently will be able to bring a phone to school and this is done so at theirs and their parents' own risk. Shelton Junior School cannot be held responsible for property brought onto the school premises.

Staff must leave their mobile phones in the Staff Room.

The sending of abusive or inappropriate text messages is forbidden.

Personal Data

Data Protection Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition. Actions are currently being implemented in order to ensure compliance with the new GDPR (Government Data Protection Regulation) and this policy will be updated in line with this new legislation.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice"
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the GDPR.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.
- All laptops have an automatic lock enabled after 10 minutes of no-use.

Staff ensure that they:

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Lock their laptops when leaving them unattended
- Use personal data only on secure password protected computers and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices
- Where personal data is stored on removable media:
- The data is encrypted and password protected
- The device is password protected
- The device has approved virus and malware checking software
- The data is securely deleted from the device once finished with.

Authorising Internet Access

- All staff must read and sign the Acceptable Use Agreement.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents will be asked to sign the Parent Internet agreement in the front of their child's home-school diary.

Internet risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Shelton Junior School cannot accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is effective.

Handling e-safety Complaints

- Complaints of pupil Internet misuse will be dealt with by the E-Safety Coordinator, as a first point of call. This may then be passed onto a more senior member of staff.
- All children will be taught to use the Internet safely and the role of the CEOP to monitor and report abuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of cyber-bullying are dealt with in accordance with our AntiBullying policy. Complaints related to child protection are dealt with in accordance with school child protection and safeguarding procedures.
- As each case will be different, this policy cannot offer specific advice about what should be done.
- The school believes that cyber-bullying (along with all forms of bullying) is unacceptable. All incidents of cyber-bullying reported to the school will be recorded. The school will take steps to identify bullying behaviour where appropriate.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Introducing the E-Safety policy

To staff:

- The E-Safety Policy will be formally provided and discussed with all relevant staff members. They will be required to sign and date to confirm that they have read it.

- To protect all staff and pupils, the school will implement Acceptable Use policy. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use will be provided.

To parents:

- Parents' attention will be drawn to the Shelton Junior School's E-Safety Policy in newsletters and on the school website.
- A partnership approach with parents will be encouraged. This will include parent meetings with demonstrations and suggestions for safe home Internet use.
- Parents will be requested to sign an e-safety agreement form. Information and guidance will be made available to parents in a variety of formats.
- Parents will be requested to sign a ClassDojo permission from to allow their child's photo to be posted on ClassDojo.

To pupils:

E-Safety rules will be displayed in all classrooms where computers are used. As they progress through the school, children will be taught these SMART rules (from Childnet), as part of an on-going e-safety curriculum.

Safe – Keep personal information safe and secret; think carefully before you share a photo of yourself or friends.

Meeting – Don't meet up; never arrange to meet an online friend because it might be dangerous. No matter how well you think you know people, they might be pretending.

Accepting – Accepting emails can be dangerous; if you receive junk mail (called Spam) or messages which make you feel uncomfortable, tell an adult that you trust and delete them. Don't reply to them!

Reliable – the Internet is full of friendly people and amazing information. However, sometimes people might say or write things which are untrue so you should always think carefully before trusting what you see or hear.

Tell – Tell someone! Most of the time that you are online, you will have lots of fun. However, if you see something that makes you feel uncomfortable or worried, make sure that you tell an adult you trust.