Shelton Junior School

E-Safety Policy

Headteacher Approval	Governor Approval	Shelton Junior School
Name: Mr Jon Bacon **Date:** 25/03/2021	**Name:** Ms K Phillips **Date:** 25/03/2021	*E-Safety Policy* Last Reviewed: March 2021 Review date: March 2022

Policy review dates and changes

Date	By whom	Summary of changes made
15/01/2020	JB	Removed author
15/01/2020	JB	Formatting and pagination corrections
15/03/2021	DB	Policy review

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

- This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- It also refers to the DfE's guidance on protecting children from radicalisation.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- The policy also takes into account the National Curriculum computing programmes of study.

3. Statement of Intent

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 Computer-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.

3.1 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.

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

3.2.1 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 (e.g. racist, radical and extremist views)
- Content validation: how to check authenticity and accuracy of online content (fake news)

3.2.2 Contact:

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

3.2.3 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)

4. Roles and responsibilities

4.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular safeguarding meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

4.2 The Head teacher

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Pastoral & Safeguarding Lead

Details of the school's DSL and DDSL are set out in our child protection and safeguarding policy.

The Pastoral & Safeguarding Lead takes lead responsibility for online safety in school, in particular:

- Supporting the Head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head teacher, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged onto CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety in conjunction with the Computing Lead
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head teacher and/or governing board
- Acting as the named point of contact within the school on all online safeguarding issues.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure for a concern.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

4.4 The Computing Subject Leader

Taking the lead responsibility for online safety in the school.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND and vulnerable learners face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and Safeguarding Lead
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety.
- Working with the Head teacher, Safeguarding Lead and governing board to update this policy on a regular basis.
- Examine emerging technologies for educational benefit and carry out a risk assessment before use in school is allowed.
- Designing and creating an eSafety curriculum, in line with the National Curriculum, suitable for all learners

4.5 ICT provider

The ICT provider is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

4.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.

- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged onto CPOMs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

4.7 Pupils

- Respect the feelings and rights of others both off and online.
- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff or a trusted adult if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Responsible for contributing to the development of online safety.

4.8 Parents

Parents are expected to:

- Notify a member of staff or the Head teacher of any concerns or queries regarding this policy.
  Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems.
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
  - What are the issues? - UK Safer Internet Centre
  - Hot topics - Childnet International
  - Parent factsheet - Childnet International
  - Healthy relationships – Disrespect Nobody
  - Parent guide to apps, games and social media sites: NSPCC Net Aware

4.9 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Educating pupils about online safety

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. Online safety teaching is always appropriate to pupils' ages and developmental stages.

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE including RSE
- Computing

All children are taught to think SMART:

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 messages 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.

5.1 The National Curriculum

The text below is taken from the National Curriculum computing programmes of study.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*

- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

5.2 Education for a Connected World

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance. The Education for a Connected World framework describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

The document supports one of the key aims of the government's Internet Safety Strategy of supporting children to stay safe and make a positive contribution online, as well enabling teachers to develop effective strategies for understanding and handling online risks.

Areas of coverage:

- Self-image and identity
- Online reputation
- Online bullying
- Online relationships
- Managing online information
- Privacy and Security
- Copyright and Ownership
- Health, well-being and lifestyle

5.3 Special Educational Needs and Disability (SEND)

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO, DDSL and Computing Lead work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

6. Cyberbullying

6.1 Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyberbullying

- To help prevent cyberbullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyberbullying to parents via Class Dojo so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
- The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.
- Concerns regarding online peer-on-peer abuse are reported to the DSL/DDSL who will investigate the matter with other senior colleagues.

7. Staff Training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction. Online safety training for staff is updated regularly and is delivered in line with advice from local and national safeguarding partners. In addition to this training, staff also receive regular online safety updates as required and at least annually from the DDSL and/or Computing Leader. The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media. All staff are informed about how to report online safety concerns.

8. Educating parents and carers

- The school works in partnership with parents to ensure pupils stay safe online at school and at home.
- Parents are provided with information about the school's approach to online safety and their role in protecting their children.
- This information is sent out via E-mail, Newsletters and Class Dojo. Parents are also given a copy of the Acceptable Use Agreement to ensure their child understands the document and the implications of not following it.

9. Classroom use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law. Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

10. Internet access

- Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.
- A record is kept of users who have been granted internet access in pupil electronic file.
- All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

11. Filtering and monitoring online activity

- The ICT Provider ensures the school's ICT network has appropriate filters and monitoring systems in place.
- The ICT Provider and Headteacher undertake a risk assessment to determine what filtering and monitoring systems are required.
- The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.
- Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, Headteacher and the ICT provider conduct a risk assessment.
- Any changes made to the system are recorded by the ICT Provider.
  Reports of inappropriate websites or materials are made to DSL/DDSL immediately, who investigates the matter and makes any necessary changes.
- Deliberate breaches of the filtering system are reported to the DSL/DDSL and Computing Leader, who will escalate the matter appropriately and track trends.
- If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.
- If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
- The school's network and school-owned devices are appropriately monitored.
- All users of the network and school-owned devices are informed about how and why they are monitored.

12. Network/Server security

- Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT Provider.
- Firewalls are switched on at all times.
- The ICT Provider reviews the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.
- Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.
- Staff members and pupils report all malware and virus attacks to the ICT Provider.
- All members of staff have their own unique usernames and private passwords to access the school's systems.
- Pupils are provided with their own unique class username and passwords.
- Staff members and pupils are responsible for keeping their passwords private.

- Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.
- Users are required to lock access to devices and systems when they are not in use.
- Users inform the ICT Provider if they forget their login details, who will arrange for the user to access the systems under different login details.
- If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

13. Personal Data

Data Protection Personal Data is defined as any data which relates 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

14. Transfer of Data

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.

- Secure Cloud Services such as 'One Drive' and 'Microsoft Teams' are used by staff to securely store documents.
- 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.

15. E-mails

- Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and the Schools Code of Conduct Policy.
- Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.
- Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use agreement.
- Personal email accounts are not permitted to be used on the school site.
- Any email that contains sensitive or personal information is only sent using secure and encrypted email.
- Staff members and pupils are required to block spam and junk mail, and report the matter to the ICT provider.
- The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.
- Chain letters, spam and all other emails from unknown sources are deleted without being opened.
- Through the curriculum, children will learn what a phishing email and other malicious emails might look like.

16. Social Networking

- Access to social networking sites is filtered as appropriate.
- Staff and pupils are not permitted to use social media for personal use during lesson time.
- Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

- Staff receive regular training on how to use social media safely and responsibly.
- Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.
- Pupils are taught how to use social media safely and responsibly through the online safety curriculum.
- Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.
- The school's official social media channels are only used for official educational or engagement purposes.
- Staff members must be authorised by the headteacher to access the school's social media accounts.
- Our school uses Class Dojo to communicate with parents and carers. Teaching staff can post on these technologies.
- All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.
- The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.
- 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 there are concerns 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.

17. 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 class teacher at registration and be given back at the end of the 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. The school store the mobile devices in a secure space in the main office.

- Shelton Junior School cannot be held responsible for property brought onto the school premises.
- Staff must leave their mobile phones in their personal lockers.
- The sending of abusive or inappropriate text messages is forbidden.

18. 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 Computing Coordinator will take overall editorial responsibility and audit the website to ensure that content is accurate and appropriate. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

18.1 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. Parents will be requested to sign a Class Dojo permission form to allow their child's photo to be posted on Class Dojo.

19. Authorising Internet Access

- All staff must read and sign the Acceptable Use Agreement. Discretion and professional conduct is essential.
- 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.
- 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 and give permissions for photos (e.g. website and Class Dojo)

20. Handling E-Safety Complaints

- Complaints of pupil Internet misuse in school will be dealt with by the Computing Lead, which 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 Anti-Bullying policy. Complaints related to child protection are dealt with in accordance with school child protection and safeguarding procedures.

- 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.