STRATFORD PRIMARY SCHOOL

Online Safety Policy

Date adopted by Governors:	March 2023
Date for policy review:	March 2024
Person responsible	Computing Lead
Signed by Chair of Governors	March 2023

Introduction

"The internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom"

Online Safety encompasses not only internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children, young people and adults about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory National Curriculum and a necessary tool for learning. It is an essential element for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access.

Policy Aims

This online safety policy has been written by Stratford Upon Avon Primary School and takes into account the DfE statutory guidance 'Keeping Children Safe in Education', 'Early Years and Foundation Stage' and 'Working Together to Safeguard Children'

Policy Purpose

The purpose of this policy is to:

- Safeguard and protect all members of our school community online.
- Identify approaches to educate and raise awareness of online safety throughout
- the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material.
- **Contact:** being subjected to harmful online interaction with other users.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. (Appendix 1 & 2)

Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- We know that the internet and associated devices, such as computers, laptops, tablets, mobile phones and games consoles, are an important part of everyday life.
- We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Anti-bullying policy
- Staff Code of Conduct policy
- Behaviour policy
- Child protection policy

Monitoring and Review

- Technology in this area evolves and changes rapidly. This school will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head and Safeguarding team will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding, will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Mrs Gill Humphriss, has lead responsibility for online safety. Whilst activities of the Designated Safeguarding Lead may be delegated to an appropriately trained deputy (Tracey Parton, Lisa Chisholm and Anna Slater) the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

The Strategic Leadership Team:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety;
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The DSL / Safeguarding Team will:

- Identify a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.

- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the Governing Body.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Encourage their children to adhere to school policies
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and other related policies

- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Awareness and engagement with parents and carers

We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. This takes on additional significance in regard to remote education and the extra time being spent online as a consequence of the pandemic. We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats which can include highlighting online safety at other events such as parent evenings, newsletters, the website and online safety sessions.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our policies and discuss the implications with their children.

Teaching and Learning

Online safety should be a focus in all areas of the curriculum and staff reinforce online safety messages in the use of computing across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet as part of a lesson, e.g. using search engines on laptops or iPads, staff must be vigilant in monitoring the content of the websites that are accessed as a result of these searches.
- It is accepted that from time to time, for educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (ICT Development Service / ICTDS) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils are taught in all lessons to be critically aware of the content they access online and are guided to validate the accuracy of information (In relation to Online Safety curriculum overview)
- Pupils are taught to acknowledge the source of information used and respect copyright when using material accessed on the internet

- Email, online history and VLE communications are monitored
- Users must immediately report, to the DSL / Safeguarding Team – 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 communication
- Any digital communication between staff and 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.

Safer Use of Technology

We use a wide range of technology. This includes access to:

- Laptops, chrome books, iPads and other digital devices
- Internet which may include search engines and educational websites.
- Digital cameras, web cams and video cameras
- All owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- No app can be downloaded on individual pupil devices and internet access is filtered.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school's filtering levels ensure all content is appropriate for the intended audience.

Supervision of learners will be appropriate to their age and ability.

- (Early Years Foundation Stage and Key Stage 1's use of internet will be by adult demonstration, with supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
- Key Stage 2 learners will use age-appropriate search engines and online tools. Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the age and ability.

Managing Internet Access and filtering:

- The ICTDS team use Smoothwall's filtering system for all devices in Stratford Upon Avon School, by using wireless authentication to connect users to their secure BYOND Network. The filtering system is sometimes referred to as the
- Warwickshire School's Gateway
- Virus protection is installed and updated regularly
- Security of the school information systems is reviewed regularly by the ICTDS

- The Online Safety Co-ordinator and IT School Support Technician meet regularly to ensure filtering systems are in place and up to date
- The school uses the Warwickshire Broadband with its firewall and filters
- The school provides an additional level of protection through its deployment of Policy Central in partnership with Warwickshire ICTDS. This software monitors text appearing on the screen and keyboard input, identifying the use of words that are included on a list of 'banned words'. The software captures the screen, identifying machine and user details so appropriate action can be taken.

Use of Email

- The school is provided with a login, password and email account for each pupil on entry to Stratford Upon Avon Primary School.
- Stratford Upon Avon Primary School do not currently use the email account, which is linked to Warwickshire's 365 learning platform, and do not provide pupils with the email address. Pupils are encouraged to communicate with teachers and pupils via the discussion groups and messaging services on the VLE.

Published content and the school website

- The contact details on the school's website should be the school address, email and telephone number. Staff or pupil's personal information will not be published.

Publishing pupils' images:

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name (teachers are aware of pupils that should not be photographed for publication purposes)
- Written permission from parents or carers is obtained annually before photos of pupils are used for any purpose relating to the school.

Learners Personal Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.

- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Learners will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

Staff and the Online Safety Policy

- All staff are given the school's Online Safety Policy
- Staff members are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- An online safety training meeting for staff members is held annually to raise the awareness and importance of safe and responsible Internet use.

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraudhttps://www.actionfraud.police.uk/.police.uk
- Child Exploitation and Online Protection:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

List of Acronyms

DSL- Designated Safeguarding Lead

ICTDS - ICT Development Services

VLE- Virtual Learning Environment

Appendix 1

Acceptable User Policy for Stratford upon Avon Primary School

This is how we stay safe when we use the internet and other personal electronic devices, when at school and outside of school:

- I will ask an adult if I want to use the computer.
- I will only use activities that an adult has told or allowed me to use.
- I will take care of any electronic devices that I use.
- I will ask for help from an adult if I am not sure what to do or think I may have done something wrong.
- I will tell an adult if something upsets me or is inappropriate.
- I know that if I do not follow these rules I might not be able to use electronic devices in the future.
- I must check the age that I have to be before I use websites, apps, software, DVD's and games.
- I will never send offensive messages when using electronic devices.
- I will not access other people's information when using electronic devices.

Signed (child): ……

Signed (adult): ……..

Appendix 2:

Acceptable use agreement
(staff, governors, volunteers and visitors)

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):
Date: