	South Bersted CE Primary E-Safety Policy
Web and/or Internal	**Web & Internal**
This policy should be reviewed every	**Every three years**
Policy approved by Governors	**Autumn 2020**
Date of Review	**Autumn 2023**
Member of staff responsible	**Headteacher**
Policy created by	**WSCC Model Policy, personalised**
Signed by Chair of Governors and/or Headteacher	

Introduction

At South Bersted Church of England Primary School, our vision states, 'pupils are encouraged to embrace challenges and become lifelong learners in a safe, secure and nurturing environment.' Our aim in presenting an e-safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.

E-safety is not purely a technological issue. The responsibility for e-safety must not be solely delegated to technical staff, or those with a responsibility for ICT. Therefore, at South Bersted Church of England Primary School we firmly embed e-safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

No one policy or technology can create the safe learning and working environment we need. At South Bersted, we work towards this by combining the following:

1. **Policies** and Guidance.
2. **Technology** Based Solutions
3. **Education** in terms of acceptable use and responsibility

Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

- The school Acceptable Use Policy (AUP)

- The school Internet Filtering Policy
- The staff Guidance for the Safer Use of the Internet
- The Information Security Guidance

These policies set the boundaries of acceptable use in conjunction with other policies including, but not limited to:

- The Behaviour Management Policy
- The Anti-Bullying Policy
- The Staff Handbook / Code of Conduct for Staff
- Data Protection Policy

Technology

The technologies to help form a safe environment to learn and work include:

- Internet filtering
- Antivirus Software - regularly updated.

Roles and Responsibilities:

At South Bersted Church of England Primary School, the Headteacher and Governors have ultimate responsibility to ensure that this policy and the practices are embedded and monitored. The named e- Safety coordinator for the school is Noel Goodwin. The school's computing and PSHE leads, have responsibility to ensure curriculum delivery of e-safety. All members of staff have been made aware of who holds this post. It is the role of the e-safety coordinator to remain up to date with current issues and guidance.

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 have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction;
- all digital communications with and regarding students / pupils / parents / carers should be on a professional level;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the Online Safety Policy and acceptable use policies;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current 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.

Designated Safeguarding Lead:

Designated Safeguarding Leads should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

As these are safeguarding issues, records and trends will be monitored to ensure training and curriculum needs are adapted to meet the children's and staff's needs.

The 360° safe - the e-safety self-review tool:

At South Bersted Church of England Primary School, the 360° safe self review tool (provided by the South West Grid for Learning) is used. This tool is reviewed annually by the DH, SBM and the computing subject leader, to provide the following:

- management information that can help the production or review of e-safety policies and develop good practice,
- a process for identifying strengths and weaknesses in the school's policies and practices,
- opportunities for commitment and involvement from the whole school,
- a platform for the school to discuss how it might move from a basic level provision for e-safety to practice that is aspirational and innovative.

Training:

On induction to the school, all staff and volunteers will receive online safety training. In addition to this, as part of the school's approach to safeguarding, staff will receive online safety updates and training throughout the year.

The school's identified Safeguarding Governor and other members of the Full Governing Body, will also complete online safety training. They may also attend information sessions for staff or parents (this may include attendance at assemblies / lessons).

Education:

The education of young people is key to them developing an informed confidence and resilience that they need in the digital world.

The National Curriculum programme for computing at Key Stages 1 to 4 makes it mandatory for children to be taught how to use ICT safely and securely. Together, these measures form the basis of a combined learning strategy that can be supported by parents, carers and the professionals who come into contact with children.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience. At South Bersted Church of England Primary School, we continually look for new opportunities to promote e-safety:

- we provide opportunities within the computing and PSHE curriculum areas to teach pupils about online safety, including responding to and managing online relationships,
- educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum,

- pupils are taught about copyright and respecting other people's information, images, through discussion, modelling, and activities as part of the Computing and PSHE curriculums,
- pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying),
- pupils are taught to critically evaluate materials and learn good searching skills through the school's Computing Curriculum,
- pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know.

The school actively engages in Safer Internet weeks, which are organised by the school's Computing lead.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, young people must be able to transfer established skills and safe working practices to any new "e-activities" they encounter.

We recognise that it is equally important to ensure that the people who care for young people should have the right information to guide and support young people whilst empowering them to keep themselves safe.

Working in Partnership with Parents:

Parents/carers are asked to read through and sign 'Acceptable use of ICT Agreements' on behalf of their child on admission to school (Appendix B).

As part of the school's approach to supporting parents:

- parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website)
- a partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use,
- advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents via the school's website and parent communications including the school's newsletter.

Managing Internet Access:

Through the school's acceptable use polices: KS 1 pupils, KS 2 pupils and staff, the school has a clear record of all pupils and adults that have access to the school's internet.

Use of visitors; only known professionals using their work devices within the school setting are given the school wi-fi code.

For further information see the school's Acceptable Use Policies.

Use of Passwords:

All members of staff have their own unique username and private password to access the school's systems. Staff are responsible for keeping their passwords private.

At South Bersted Church of England Primary School, pupils across the school use a class password

to access the school's Learning Drive. When accessing websites which require a log in, pupils across the school are provided with their own user name and password. Users are responsible for the security of their username and password.

When using the school's Chrome Books and or accessing their own accounts we require all users to:
Use strong passwords: including a character and a number,
Keep their passwords private,
Not to login as another user at any time,
Tall an adult if they feel their password has been compromised.

Filtering and monitoring:

Education broadband connectivity is provided by EXA through JSPC.
The school uses Surf Protect Cloud to ensure that pupils are kept safe online, whilst letting them access useful websites, resources and tools.
The school works alongside JSPC to ensure that the school's filtering policy is continually reviewed.
If pupils discover unsuitable sites, they are required to:

- Turn off the monitor or screen and report the concern immediately to a member of staff.
- The member of staff must then report the concern along with the ULR of the site to the named e-safety coordinator: Mr Goodwin.
- The breach will be recorded (see Appendix A) and escalated as appropriate.
- Parents/ carers will be informed of the filtering breach involving their child.

For further information on filtering, refer to South Bersted's Filtering Policy.

Use of images:

Refer to the school's use of images policy which outlines in detail the school's requirements in obtaining parental permission to ensure all children and staff are safeguarding effectively.

Responding to e-safety incidents of misuse:

As a school we will take all reasonable precautions to ensure e-safety. There are clear systems in place for recording and responding to e-safety concerns and incidents of misuse.

Any incidents of misuse will be reported as part of the headteacher's report.

Cyberbullying:

Cyberbullying, along with other forms of bullying will not be tolerated at South Bersted Church of England Primary School. Full details of how the school responds to cyberbullying are set out in the school's anti-bullying policy.

Online Hate:

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at South Bersted Church of England Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures and the Police will be contacted if a criminal offence is suspected.

Online Radicalisation and Extremism:

As a school, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.

If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

National Links and Resources for Educational Settings:

CEOP:www.thinkuknow.co.uk, www.ceop.police.uk
Childnet: www.childnet.com
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
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers:

Action Fraud: www.actionfraud.police.uk
CEOP: www.thinkuknow.co.uk
Childnet: www.childnet.com
Internet Matters: www.internetmatters.org
NSPCC: www.nspcc.org.uk/onlinesafet
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk

Appendix A

South Bersted C.E Primary School

E-Safety Incident Report Form

Reporting Adult:	Date:
Details of e-safety incident:	
Where did the incident occur? (school (room) or home)	
Who was involved in the incident? Pupil's name: _____ Name of staff member/ volunteer: _____	
Description of incident (including IP address, relevant user names, devices, programmes and context).	
Action Taken: ☐ Incident reported to the headteacher/ SLT ☐ Advice sought from DSL ☐ Incident reported to BM and the site is blocked ☐ Disciplinary action to be taken ☐ E-safety policy reviewed ☐ Parents/ carers informed. Other:	
Outcome of the incident:	