St Paul's C of E (VC) Junior School

"Promoting, Valuing and Celebrating achievement in a Christian setting."

ICT/E-Safety Policy

Date: ……Spring 2017……..

Review Date: …Spring 2018…….

Author: ……David Fingleton……

Approved by Governors: …….

"Prevent Duty: Under section 26 of the Counter-Terrorism and Security Act 2015, we have a duty to prevent people from being drawn into terrorism (Prevent duty). Protecting children from the risk of radicalisation remains part of our school's wider duty to safeguard children and young people. "*Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism....Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and* tolerance *of different faiths and beliefs." (KCSIE, September 2016)*. We are alert to any possible signs which contribute to vulnerability such as family, friends or online influences as well as any changes in behaviour which could indicate a child may be in need of help or protection. We carry out risk assessments of vulnerable children and young people accordingly, work in partnership with other agencies and the family, and ensure staff are suitably trained and supported in keeping with our LSCB procedures."

This policy is written with reference to the Christian Foundation of the school and to the school's Christian values of Respect, Equality, Friendship, Love, Encouragement, Compassion and Trust.

This policy is written with reference to the Rights of the Child
Article 19: the right to be protected from being hurt or mistreated, in body and mind.
Article 36: the right to be protected.

This policy is written in conjunction with the Safeguarding, Mobile Phone and Acceptable User policies.

The e-Safety policy sets out the framework and expectations that all staff, learners and St Paul's CofE VC Junior School community should adhere to in respect to the use of computing equipment, the internet and all forms of electronic communication such as email, mobile phones, social media sites and related learning technologies.

The e-Safety policy is designed to detail the principles all users should adhere to when using these services. This guidance does not attempt to cover every possible situation but should be used as a supporting framework in relation to e-Safety.

Introduction

St Paul's CofE VC Junior School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide safe and secure internet access to all learners and staff and encourage the use of ICT and learning technologies in order to enhance skills, promote achievement and enable lifelong learning and world class outcomes.

However, the accessibility and global nature of the internet and associated learning technologies that are available mean that we all need to be aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks safely, independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and the implementation of the relevant policies. In addition to our duty to safeguard staff and learners, we will do all that we can to make our staff and learners e-Safe and to satisfy our wider duty of care.

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology;
- Build both an infrastructure and culture of e-Safety;
- Work to empower the school community to use the Internet as an essential tool for life-long learning.

Scope of policy

The e-Safety policy applies to all users, learners, staff and all members of St Paul's CofE VC Junior School community who have access to the school ICT systems, both on the premises and remotely. Any user of the school ICT systems must adhere to and sign a hardcopy of the Acceptable Use Policy. The e-Safety Policy applies to all use of computing equipment (fixed and mobile), the internet and all forms of electronic communication such as email, mobile phones and social media.

The school will manage e-Safety as described within this policy and associated safeguarding policies, and will inform parents and carers of known incidents of inappropriate e-Safety behaviour that take place in and out of school.

Roles and Responsibilities

Designated e-Safety Lead	David Fingleton	Lead the e-Safety working group Log, manage and inform others of e-Safety incidents Lead the establishment and review of e-Safety policies and documents Ensure all staff are aware of the procedures outlined in policies relating to e-Safety Provide training and advice for staff Attend updates and liaise with the LA e-Safety staff and technical staff Meet with Senior Leadership Team and e-Safety Governor to regularly discuss incidents and developments Coordinate work with the school's designated Child Protection Coordinator
Designated Child Protection Lead	Christopher Partridge Sally Jefferies Karen Francis Tracey Roberts	Ensure that all staff receive suitable CPD to carry out their e-Safety roles Create a culture where staff and learners feel able to report incidents Ensure that there is a system in place for implementing e-Safety Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil Inform the local authority about any serious e-Safety issues Ensure that the school infrastructure/network is as safe and secure as possible Ensure that policies and procedures approved within this policy are implemented Use an audit to annually review e-Safety with the school's technical support
Link Governor	Hayley Green (Safeguarding) Albert Owen (Chair)	Approve and review the effectiveness of the e-Safety Policy Works with the e-Safety lead to carry out regular reviews and report to Governors
Education Safeguarding Advisor	Jane Weatherill (SSE)	
Teaching and Support Staff		Participate in any training and awareness raising sessions Read, understand and sign the Staff AUP Act in accordance with the AUP and e-Safety Policy Report any suspected misuse or problems to the e-Safety lead Monitor ICT activity in lessons, extracurricular and extended school activities
Pupils		Participate in e-Safety activities, follow the AUP and report any suspected misuse Understand that the e-Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers		Discuss e-Safety issues with their children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Access the school website in accordance with the relevant school AUP Keep up to date with issues through newsletters and other opportunities Inform the Headteacher of any e-Safety issues that relate to the school
Technical Support Provider	Computeam	Ensure the school's ICT infrastructure is as secure as possible Ensure users may only access the school network through an enforced password protection policy for those who access children's data Maintain and inform the Senior Leadership Team of issues relating to filtering Keep up to date with e-Safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-Safety Leader for investigation Ensure monitoring systems are implemented and updated Ensure all security updates are applied (including anti-virus)
Other Users		Sign and follow the Staff AUP before being provided with access to school systems

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to the e-Safety Officer. All teaching staff are required to adhere to this incident reporting procedure.

When informed about an e-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All learners must know what to do if they have e-Safety concerns and who to talk to. In most cases, this will be the e-Safety lead or the Child Protection lead. Where any report of an e-Safety incident is made, all parties should know what procedure is triggered and how

this will be followed up. The Child Protection Officer may be asked to intervene with appropriate additional support from external agencies.

e-Safety Lead

The e-Safety leader is responsible for keeping up to date with new technologies and their use, as well as attending any relevant training. The e-Safety lead will be expected to review the e-Safety Policy, deliver staff development and training, deliver workshops for parents, manage the reporting procedure, record incidents, report any developments and liaise with the Senior Leadership Team and external agencies to promote e-Safety within St Paul's CofE VC Junior School.

Staff

All staff are responsible for using the school ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy and the AUP policy which they must sign. Staff must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. Staff are responsible for attending training on e-Safety and displaying a model example to learners at all times through embedded good practice.

Any digital communications with parents, learners and external agencies must be professional at all times.
All staff should adhere to the relevant school policies detailed in the e-Safety Policy and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the e-Safety lead and/or designated child protection lead without delay. Please use form attached as Appendix A, supplies can be found in the Staff Room. (Please use in conjunction with the Blue Safeguarding form, if required.)

Security

St Paul's CofE VC Junior School will do all that it can to make sure the school ICT network and systems are safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of filtering and firewalls for servers, routers, and all school provided user devices (desktop/laptop/tablet/mobile etc.) to prevent accidental or malicious access of school systems and information.

Digital communications, including the school network, email systems and document storage may be monitored.
It is recommended for security purposes that all user account passwords be changed on a 45-60 day cycle where practicably possible.

Schedule for Development, Monitoring and Review

The Implementation of the e-Safety policy will be monitored by a working group (e-Safety lead, Child Protection lead, link governor) meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the e-Safety working group by looking at:

- Log of reported incidents
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

The e-Safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to e-Safety or incidents that have taken place.

Education of pupils

With the current unlimited nature of internet access, it is impossible for St Paul's CofE VC Junior School to eliminate all risks for staff and learners. It is our view therefore, that the School will support staff and learners to stay e-Safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

A progressive planned e-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

- Key e-Safety messages are reinforced through assemblies and Safer Internet Week (February) and throughout all lessons.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will write and sign an AUP for their class at the beginning of each school year, which will be shared with parents and carers.

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing e-Safety risks at home, reinforcing key messages about e-Safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children and regular newsletter and web site updates;
- Inviting parents to attend activities such as e-Safety workshops, e-Safety assemblies or other meetings as appropriate.

Training of Staff and Governors

There is a planned programme of e-Safety training for all staff and governors to ensure they understand their responsibilities. This includes:

- An annual audit of the e-Safety training needs of all staff.
- All new staff receiving e-Safety training as part of their induction programme.
- The e-Safety lead receiving regular updates through attendance at LA training sessions and by reviewing regular e-Safety newsletters from the LA.
- This e-Safety Policy and its updates being shared and discussed in staff meetings.
- The e-Safety lead providing guidance and training as required to individuals and seeking LA support on issues.

- Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772.

Technical Infrastructure

The person(s) responsible for the school's technical support will sign a staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets e-Safety technical requirements.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

    - The downloading of executable files by users.
    - The extent of personal use that users (staff/pupils users) and their family members are allowed on laptops and other portable devices used out of school.
    - The installing of programs on school devices unless permission is given by the technical support provider or ICT coordinator.
    - The use of removable media by users on school devices.
    - The installation of up to date virus software.

- Access to the school network and internet will be controlled with regard to:

    - Users having clearly defined access rights to school ICT systems.
    - Users being provided with a username and password.
    - Users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details.
    - Users must immediately report any suspicion or evidence that there has been a breach of security.
    - An agreed process being in place for the provision of temporary access of "guests" (e.g. supply teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this e-Safety policy.
    - Pupils will be supervised. Pupils will use age-appropriate search engines and online tools and activities which will be adult directed.

- The internet will be controlled with regard to:

    - The school maintaining a managed filtering service provided by an educational provider.
    - The school monitoring internet use.
    - Requests from staff for sites to be removed from the filtered list being approved by the Headteacher.
    - Any filtering issues being reported immediately to SWGfL helpline.

- The ICT System of the school will be monitored with regard to:

    - The school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems.
    - e-Safety incidents being documented and reported immediately to the e-Safety lead who will arrange for these to be dealt with immediately in accordance with the AUP.

Data Protection

The school Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The school will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices.
- Ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data.
- Make sure data is deleted from the device once it has been transferred or its use is complete.

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers and to provide information about the school on the website.
The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils' full names will not be used anywhere on the school website or other platforms, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.
- Not publish pupils' work without their permission and the permission of their parents.
- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.
- Adhere to the schools policy on acceptable use of photographic images.

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

- Email
    - Ensure that all school business will use the official school email service.
    - Ensure that any communication between staff and pupils or parents and carers is professional in tone and content.
    - Make users aware that email communications may be monitored.
    - Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
    - Ensure that personal information is not sent via email.
    - Only publish official staff email addresses.

- Social media
    - Control access to social media and social networking sites.
    - Have a process to approve staff who wish to use social media in the classroom.
    - Inform staff not to run social network spaces for pupil use on a personal basis.
    - Not publish information and share learning experiences on personal Facebook/Twitter accounts.
    - Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
    - Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites.
    - Outline safe and professional behaviour.

- Mobile phones (see also mobile phone policy)
    - Allow staff to bring mobile phones into school but must only use them during break, lunchtimes or during non-contact when they are not in contact with pupils' unless they have the permission of the

Headteacher. Staff and visitors are not allowed to take photographs or video in school for any purpose without the express permission of the Headteacher.
- Advise staff not to use their personal mobile phone to contact pupils, parents and carers.
- Provide a mobile phone for activities that require them.

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances St Paul's CofE VC Junior School will examine and adjust the e-Safety Policy. Consideration will include:

- Looking at the educational benefit of the technology.
- Considering whether the technology has access to inappropriate 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. The school or Somerset County Council cannot accept liability for the material accessed, or any consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

Where an e-Safety incident is reported, the school will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their teacher or to the school e-Safety lead.

Where a member of staff wishes to report an incident, they must contact the Headteacher as soon as possible. Following any incident, the school will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Serious incidents will be dealt with by the Headteacher, in consultation with appropriate external agencies.
All incidents will be recorded in accordance with the school's child protection policy. Where there is a cause for concern, the school will contact the Somerset Education Safeguarding Advisor, LADO or police.

The school will follow Somerset's Incident Flowchart to respond to illegal and inappropriate incidents.

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images.
- Promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation.
- Adult material that potentially breaches the Obscene Publications Act in the UK.
- Criminally racist material.

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography, adult or mature content.
- Promotion of any kind of discrimination, racial or religious hatred.
- Personal gambling or betting.
- Personal use of auction sites.
- Any site engaging in or encouraging illegal activity.
- Threatening behaviour, including promotion of physical violence or mental harm.

- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Using school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet.

Appendix A

E-safety Incident Report Form

This form should be kept on file and a copy emailed to Somerset's e-Safety officer at jweatherill@somerset.gov.uk

School/organisation's details:

Name of school/organisation: St Paul's CofE (VC) Junior School

Address: Paul Street, Shepton Mallet, Somerset BA4 5LA

Name of e-safety contact officer: Mr D. Fingleton

Contact details: 01749 343250 dfingleton@educ.somerset.gov.uk

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ Bullying or harassment (cyber bullying)
□ Deliberately bypassing security or access
□ Hacking or virus propagation
□ Racist, sexist, homophobic religious hate material
□ Terrorist material
□ Drug/bomb making material
□ Child abuse images
□ On-line gambling
□ Soft core pornographic material
□ Illegal hard core pornographic material
□ Other (please specify)

Description of incident

Nature of incident

Deliberate access

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ cyber bullying □ breach of AUP

Accidental access

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

Staff

□ Incident reported to head teacher/E-Safety lead
□ Advice sought from Safeguarding and Social Care
□ Referral made to Safeguarding and Social Care
□ Incident reported to police
□ Incident reported to IT provider (Computeam)
□ Disciplinary action to be taken
□ e-Safety policy to be reviewed/amended

Please detail any specific action taken (i.e.: removal of equipment)

Child/young person

□ Incident reported to head teacher/ E-Safety lead
□ Advice sought from Safeguarding and Social Care
□ Referral made to Safeguarding and Social Care
□ Incident reported to police
□ Incident reported to social networking site
□ Child's parents informed
□ Disciplinary action to be taken
□ Child debriefed
□ year group/whole school assembly
□ e-Safety policy to be reviewed/amended

Outcome of incident/investigation