St Andrew’s CE VC Primary School

A church school that learns, grows and achieves together

“Train up a child in the way he should go,
and when he is old he will not depart from it”
Proverbs 22:6

E-Safety Policy

Signed (Chair)	Name Derek Jones	Date
Signed (Head)	Name Helen Green	Date
Ratified by Governing Body on		Next Review

Equality Impact Assessment (EqIA)

This policy has been assessed with regard to its impact on equalities issues. The equality impact assessment has been conducted by the relevant Governors’ sub-committee and focused on race, gender, disability, age, sexual orientation, gender identity and religion/belief. Community Cohesion has also formed part of the impact assessment work in order to ensure respect for diversity, alongside a commitment to common and shared bonds.

EqIA outcomes

□ *The assessment found no areas of potential negative impact and actions resulting in positive impact are in place.*

E-Safety Policy

Scope of the Policy

This policy applies to all members of the school community (including volunteers, parents/carers, visitors and community users) who have access to or use school ICT systems inside and outside school. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents, including cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of known incidents of inappropriate online safety behaviour that take place out of school. The 2011 Education Act increased these powers with regard to searching for and of electronic devices and the deletion of data and related action can only be taken over issues covered by the school behaviour policy.

This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour policy.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it.
- The Head teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Leader. The head teacher is also the designated person for child protection and is trained in e-safety issues and aware of the potential for serious child protection 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 and cyber-bullying.

Training and Awareness Raising

There is a planned programme of e-safety training for all staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- The Child Protection and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL and LA training sessions and by receiving regular e-safety updates from the South Gloucestershire Traded Services.
- All staff, including support staff, receive e-safety updates as necessary.

- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The ICT Subject Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.
- A training log is used to record when updates and training are delivered.

Induction Processes

- All new staff members receive online safety training as part of their induction programme.
- Parents of new reception children receive a briefing about online safety and processes when their child starts school. There are also updates to this throughout the key stages.
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.

Teaching and Learning/ Curriculum Provision

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. There is a planned and progressive scheme of work for online safety which is taught at every year group. This is based around the South Gloucestershire scheme of work and Digital Literacy Curriculum by SWGfL and, across the key stages, it covers:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self- image and identity
- Digital footprint and reputation
- Creative credit and copyright

The following aspects also contribute to our curriculum provision:

- Opportunities to reinforce this are mapped to other subjects in the curriculum where appropriate for example, online behaviour is covered in PSHE and communication, copyright and publishing may be referenced in literacy.
- Assemblies may be used to reinforce online safety messages.
- Annual online safety events such as Safer Internet Day are also used to raise awareness.

Regular opportunities are taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages are also reinforced through other subjects and through a planned programme of other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the AUP, recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children).

Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

If there are educational reasons why a blocked site is needed for learning then staff can request that this be made available to technical staff. Where this is done it is clearly logged with reasons given for this access.

Children new to the school are provided with an overview of expectations when they start. The following aspects also contribute to our curriculum provision:

- Coverage of learning experiences is recorded and staff members check understanding when teaching about online safety.
- Annual online safety events such as Safer Internet Day are also used to raise awareness.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff will refer to these as needed, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Education- Parents/ Carers and the school community

Parents and carers have an essential role in educating their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues and underestimate the dangers or be unsure how to deal with them.

The school aims to raise awareness and support parents through:

- Curriculum activities
- Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these
- Parents / carers information sessions
- Events such as Safer Internet Day
- Providing information and web links about where to access support on the website or newsletter

Parents of children new to the school are provided with an overview of expectations linked to relevant policies including online safety when their child starts school.

Education- Staff and Volunteers

All staff members receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- An audit of online safety training needs of staff is carried out regularly.
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The online safety lead receives regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.
- The online safety lead provides regular guidance and training to support individuals where required.

Self- Evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.
- Surveys with pupils and staff

Technical Issues

The local authority provides technical and curriculum guidance for Online safety issues for all South Gloucestershire schools as well as providing direct technical support to a large number of schools.

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Traded Services and this includes a filtering service to limit access to unacceptable material for all users. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners.

Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged and documented by a process that is agreed by the Headteacher. Any filtering requests for change and issues are reported immediately to the South Gloucestershire technical team on 3838. Should anyone attempt to access illegal content this is immediately reported to the police. Illegal activity would include attempting to access:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Technical Staff- Roles and Responsibilities

Where the local authority provides technical support the “administrator” passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

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

- There are regular reviews and audits of the safety and security of school ICT systems.

- Servers, wireless systems and cabling are securely located and physical access is restricted

- All users have clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.

- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- 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.
- The school infrastructure and individual workstations are protected by up to date virus software.

The Staff AUP is in place regarding the downloading of executable files by users

- The AUPs are in place regarding the extent of personal use that users are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.

Use of Digital Images and Video

With the availability of mobile devices and tablets then taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

When using digital images, staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.

- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff to reinforce this when appropriate.
- Staff members are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.

- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied.
- Parents sign permission forms to say that they will allow images to be taken of their child and used for educational purposes.
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils names are not published on any online platform or school communication including the web site, newsletter or any social media feed, e.g. Facebook/ twitter. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' names or other information that could identify them.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the Data Protection Act. However in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Governor communications do not take place through personal email accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site that governors can access via a personal user account.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community.
- Personal opinions are not attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk.

Copyright

The school is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union
- Physical or mental health or condition

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

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

Transfer of Data

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

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing” as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.

- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the General Data Protection Regulation (GDPR)

Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

- Online safety issues are reported to the Head teacher. If these include allegations of bullying then the anti-bullying policy is followed.
- Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed.
- Staff who are targeted by bullying online report these issues to the head teacher.
- Any member of staff seeing something online that is negative about the school reports this to the head teacher.
- Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.
- Younger pupils are taught to communicate to staff if they access unsafe content and older pupils are also shown how to report online in case of incidents outside school.
- If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 3838).
- If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 3838 to ensure that this is blocked.
- Serious incidents are escalated to local authority staff for advice and guidance
    - Nick Pearce – Infrastructure, Technical and Filtering - 3838
    - Jo Briscombe – Curriculum and Policy – 3349
    - Leigh Zywek – Safeguarding and Child Protection - 5933
- For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

There are defined sanctions in place for any breaches of the acceptable use policies. Suggestions for these can be accessed in SWGfL policy template (Word version with appendices) on pages 17 – 19. Schools are advised to adapt these to suit their own circumstances.

SWGfL provide clear guidance on what to do if there are suspicions that technology may be being mis-used in order to ensure that the right evidence is collected in a way that does not put the school at risk and these are followed. Refer to SWGfL policy template page 20.

Monitoring

The school will monitor the impact of the policy using:

- Logs of reported incidents and responses.
- Monitoring logs of internet activity and any network monitoring data.
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff.
- Monitoring information about the teaching programme and coverage within the curriculum.
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them.
- The content of the web site is regularly monitored by governors and senior leaders to ensure that it complies with this policy and the acceptable use policies.
- Any other web site, such as the school friends, that is linked to the school name is also regularly monitored to ensure that the school is always presented accurately and professionally.

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and acceptable use policies E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head teacher and Senior Leaders:	Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. Ensure that there is a system in place for monitoring e-safety Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff Inform the local authority about any serious e-safety issues including filtering Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader:	Lead the e-safety working group and dealing with day to day e-safety issues Lead role in establishing / reviewing e-safety policies / documents, Ensure all staff are aware of the procedures outlined in policies Provide and/or brokering training and advice for staff, Attend updates and liaising with the LA e-safety staff and technical staff, Deal with and log e-safety incidents including changes to filtering, Meet with E-Safety Governor to regularly to discuss incidents and review the log Report regularly to Senior Leadership Team
Curriculum Leaders	Ensure e-safety is reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness raising sessions Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and e-safety policy Report any suspected misuse or problem to the E-Safety Co-ordinator Act professionally and safely when using technology Monitor ICT activity in lessons, extra curricular and extended school activities Deliver the scheme of work for online safety Use opportunities in the curriculum to reinforce online safety messages
Students / pupils	Participate in e-safety activities, follow the acceptable use policy 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	Endorse (by signature) the Student / Pupil Acceptable Use Policy Ensure that their child / children follow acceptable use rules at home Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Access the school website / Merlin in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events
Technical Support Provider	Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data Inform the head teacher of issues relating to the filtering applied by the Grid 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 / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated

	Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.