ST ALBAN'S CE (AIDED) PRIMARY SCHOOL

"Inspired to make a difference in God's world with excellence and love"

E-SAFETY POLICY

DOCUMENT INFORMATION			
Reviewed by:	Standards Committee		
Last Review:	Summer 2023	**Next Review:**	Summer 2025
Review Cycle:	2 yearly		

1. **Vision**

At St Alban's CE Primary our vision for Computing is that it is an integral part of school life, used across the curriculum to enrich the children's learning. We believe computing at St Alban's School will allow the children to become confident users of new technology, equipping them for their future education and working lives.

2. **Introduction**

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole. Whilst exciting and beneficial both in and out of the context of education, much computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Alban's Primary School, we understand the responsibility to educate our pupils on e-safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, wearable devices, camera phones, PDAs and portable media players, etc).

3. **Scope of the Policy**

This policy applies to all members of the St Alban's CE School (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of St Alban's CE School computing systems, both in and out of the school.

Headteachers are empowered, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the St Alban's CE School site, as are members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

4. **Roles and Responsibilities**

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders:

- the Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Leader. The Computing Leader is supported in this work by the school's subscription to the services of 'Online Safety UK'.
- the Headteacher (Designated Safeguarding Lead) and Deputy Headteacher (Deputy DSL) should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- the Headteacher/Senior Leaders are responsible for ensuring that the Computing Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- the Headteacher/Senior Leaders will deal with the investigation/action/sanction of an incident.
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- receive reports of e-safety incidents and ensure these are logged (CPOMS) to inform future e-safety developments.

Computing Leader:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff and ensures that the ICT service provider (Drift) carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below.
- ensures that the managed service provider is fully aware of the St Alban's CE School e-safety policy and procedures.)

Network Manager/Technical staff:

The school's network manager (Drift) is responsible for ensuring that:

- St Alban's School's technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy/Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy, is applied and updated on a regular basis.
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that they:

- have an up to date awareness of e-safety matters and of the current St Alban's CE School e-safety policy and practices.
- have read, understood and signed the St Alban's School Staff Acceptable Use Policy/Agreement (AUP).

- report any suspected misuse or problem to the Headteacher or E-Safety Coordinator for investigation / action / sanction.
- use all digital communications with pupils / parents / carers be on a professional level and only carried out using official school systems.
- ensure e-safety issues are embedded in all aspects of the curriculum and other activities.
- ensure pupils understand and follow the e-safety and acceptable use policies.

Designated Safeguarding Lead and Deputies

The DSL and DSLs will be trained in e-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
- cyber-bullying

Pupils:

- are responsible for using the St Alban's CE School digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement (Appendix 1)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies in and out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The St Alban's School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns / literature. Parents and carers will be encouraged to support the St Alban's CE School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the St Alban's CE School (where this is allowed)

5. Teaching and Learning

Managing the internet

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- St Alban's School will ensure that all staff and children are aware that the use of internet derived materials should comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school ICT system's capacity and security will be reviewed regularly.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator if this is within school.
- The Computing Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing E-mail

Pupils

- At school pupils do not currently have access to a personal e-mail.
- Whole class / group email addresses may be used at KS1 and KS2.
- Pupils must immediately tell a teacher if they receive an offensive message.
- Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone without specific permission.

Staff

When using communication technologies the school considers the following as good practice:

- Staff should use only the St Alban's CE School email service to communicate with others when in school, or on St Alban's CE School systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the St Alban's CE School policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) St Alban's CE School systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on the St Alban's CE School website and only official email addresses should be used to identify members of staff.

Managing Content

Published content and the school website

- The contact details on the website are the school address, e-mail and telephone number. Staff, Governors' or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Use of digital and video images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras and iPads to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media in line with the school's Data Protection Policy.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on the school website or blog, particularly in association with photographs.
- Photographs that include pupils will be selected carefully. Permission forms are completed by all parents when children enter the school before photographs of pupils are published on the school website. Permission lists are kept in the ICT security folder in the ICT suite.

<u>Social networking and personal publishing</u>

- Hampshire County Council blocks/filters access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that there are a variety of social network spaces outside school. While some are designed for children of primary age, others have age restrictions and therefore are inappropriate.

<u>Managing Personal Data</u>

Personal data will be recorded, processed and transferred and made available according to the school's Data Protection Policy.

<u>Managing Blogs and other learning environments (where used)</u>

- The Computing Leader and staff will monitor the usage of the Class Blogs accounts by pupils and staff regularly in all areas at least annually, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised on acceptable conduct and use when using the learning platform. This will be done through reading and signing the relevant Acceptable Use Agreement.
- All users will be mindful of copyright issues and will only upload appropriate content onto the blogs accounts.
- When staff, pupils etc leave the school their account or rights to specific school areas and blogs accounts will be removed by the School Admin Officer.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and appropriateness before use in school is allowed.
- The use of mobile phones (and wearable devices such as smartwatches) by pupils is not permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff (and the phone/device left at the school office during the school day).
- Contact with children at school should be via the school phone only.

6. Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the student/pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- 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, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff/Governors/Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will primarily be offered as follows:

- The Computing Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Computing Leader will provide advice/guidance /training to individuals as required.

7. **Technical – infrastructure / equipment, filtering and monitoring**

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- St Alban's CE School technical systems will be managed in ways that ensure that the St Alban's CE School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to St Alban's CE School technical systems and devices.
- All users (at KS2) will be provided with a username and secure password by the Computing Coordinator who will keep an up-to-date record of users and their usernames.
- The "master/administrator" passwords for the St Alban's School ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and the Computing Coordinator and kept in a secure place.
- The Computing Coordinator is responsible for ensuring that software licence logs are accurate and up to date.
- The school has provided enhanced / differentiated user-level filtering.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.
- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example One Drive, drop box, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

9. Responding to Incidents of Misuse

Internet misuse

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher. Complaints about the Headteacher must be addressed to the Chair of Governors.
- All e–Safety complaints and incidents will be recorded by the Headteacher— including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will work in partnership with staff to resolve issues.
- The Headteacher will hold discussions with the HCC Child Protection Officer to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) involving staff will be dealt with in accordance with the Staff Discipline, Conduct and Grievance Policy, Child Protection Policy and any other school policies as appropriate.

Cyber bullying

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Behaviour and Anti Bullying Policy
- There are procedures in place to investigate incidents or allegations of cyber bullying and support anyone affected by it - see the Anti-Bullying Policy
- The Headteacher is to be informed of all incidents of cyber bullying reported to the school. Incidents will be recorded in the Behaviour Log folder.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyber bullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

Blogs and other learning environments

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the blog accounts for the user may be suspended.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.
- A visitor may be invited onto the blog account by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow St Alban's CE School policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off-site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
    - **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *St Alban's CE School* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 1

St Alban's CE School Pupil Acceptable Use Policy Agreement

This is how I stay safe when I use computers:

- I will ask permission from an adult before using the Internet and ICT equipment.
- I will take care of the computers and other equipment
- I only use apps and websites that an adult has chosen.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a suitable adult if I see anything that upsets me or that I am uncomfortable with.
- I will immediately minimise and tell an adult about any webpage I not sure about.
- I will only e-mail people an adult has approved and I will send e-mails and attachments that are polite and friendly.
- I will not open e-mails sent by anyone I don't know.
- I will only use my own login and password and never give out personal information such as my home address or phone number.
- I will not access other people's files or send pictures of anyone without their permission.
- I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free.
- I will not use Internet chat rooms or arrange to meet someone I have met online.
- When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will not use mobile phones (or wearable device such as a smartwatch) in school for any reason. If I do bring a phone to school I will take the phone to the school office for the school day.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I know that if I break the rules I might not be allowed to use a computer / tablet and my parents/carers may be contacted.

Signed (child):
Signed (parent):
Date:

APPENDIX 2 – Blogging Guidelines

Blogging guidelines

St Alban's School will be introducing the use of blogging to our achievements and activities through the school year. Keeping these blogs a safe and secure place to work is very important.

The following simple guidelines will be used to keep to in order to make the most of the school blog.

- Children are to only use their first name when commenting.
- Parents who leave comments are asked to either use their first name only so as not to identify their child, or post comments as "Albert's Mum" or "Juliet's Grandfather".
- All posts will be checked by a teacher before they are published to the blog.
- All comments are moderated by the class teacher before they appear on the blog.
- Always be respectful of other people's work - be positive if you are going comment.
- No text talk - write in full sentences and read your comments back carefully before submitting.
- Everyone at St Alban's School will stick to these guidelines.