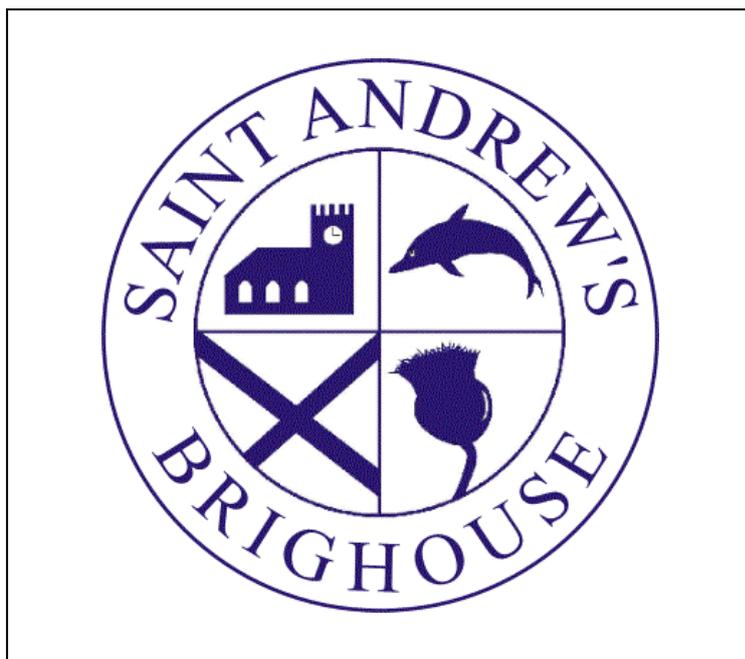


St Andrew's CE (VA) Junior School

E-safety Policy



Title	E-Safety Policy
Version	12/18
Date	September 2019
Author	Gill Meeson HR
Approved by headteacher	
Approved by governing body	
Next review date	September 2022

Contents	Page
1. Introduction.....	3
2. Purpose and scope.....	3
3. Individual roles and responsibilities	4
4. Education, internet and the curriculum.....	5
5. Managing the ICT infrastructure	6
6. School website.....	7
7. Use of ICT equipment at home.....	7
8. Use of digital and video photographic images	7
9. CCTV and monitoring	8
10. Other policies and procedures.....	8

1. Introduction

- 1.1 The aim of this policy is to set out key principles and expectations for all members of the school community with regard to the use of ICT-based technologies. The policy is designed to help safeguard and protect both students and staff in our school.
- 1.2 The relevant technologies to which the policy is applicable include, in addition to computers and associated hardware, all electronic devices including (but not limited to) mobile phones, games consoles, cameras and webcams.
- 1.3 In respect of interaction with students, management will assist staff to work safely and responsibly when utilising the internet and other communication technologies by supporting them in monitoring their own standards and practice.
- 1.4 There are clear structures in place both to minimise the risk of misplaced or malicious allegations made against staff who work with students and to deal with online abuse such as cyberbullying, sexting (sending and/or receiving personally intimate images) and identity theft including 'frape' (hacking facebook profiles).
- 1.5 Ofsted describes E-safety (in relation to schools and academies) as the ability to protect and educate students and staff in their use of technology whilst at the same time having appropriate mechanisms in place to intervene and address any incident as and when necessary.
- 1.6 This policy will be communicated to staff and students (and the wider community as and when appropriate) via school classrooms/staff rooms and website and will be an integral part of the school induction pack for new staff.
- 1.7 All members of staff in the school are encouraged (as indeed is the wider community) to exercise vigilance and to be proactive in reporting issues, in the confidence that such concerns will be dealt with quickly and sensitively through the school's escalation processes.

2. Purpose and scope

- 2.1 This policy is applicable to all members of our school community who have access to school ICT systems, both on and off school premises. This may include external contractors, trainees, volunteers, parents or carers, visitors, and community users in addition to staff and students.
- 2.2 The following extract (in relation to cyber-bullying) is taken from the DfE publication 'Preventing and tackling bullying: Advice for headteachers, staff and governing bodies' (July 2017):

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the headteacher, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

- 2.3 The principle of protecting students includes the provision of a safe learning environment by use of appropriate monitoring and filtering to control what may legitimately be accessed by students whilst at school. Essentially, however, this only protects them whilst they are on school premises. Ensuring provision of appropriate education relating to E-safety is the

only way to guarantee that, irrespective of their whereabouts, they know how to stay safe online.

- 2.4 The aim of this policy (and indeed of our school) is both to provide appropriate safeguards and to raise awareness to enable students (and others) to control their online experiences and thereby feel confident and secure in their use of technology. The entire school community needs to be fully aware of the risks (as well as the undoubted benefits) of information technology and accordingly must undertake to use it in a responsible manner.
- 2.5 Appropriate documents to serve as 'Acceptable Use Policies' (AUPs) and Loan Agreements have been developed which detail the ways in which the internet should be used and such policies (presented in this policy as appendices) are designed to be signed by students, their parents/carers, and staff.
- 2.6 Students will be instructed in the acceptable use of ICT at school, and will be given clear and principled advice and guidance for general use of mobile technologies including the internet. Appropriate objectives are made clear in the student AUPs and are displayed around the school, particularly where internet access is most frequent, such as in computer suites.
- 2.7 The E-safety policy is integrated (and consistent) with other relevant policies. These include the following: Behaviour Policy; (Staff) Disciplinary Policy; Social Media Policy; and Safeguarding Policy.

3. Individual roles and responsibilities

3.1 Headteacher

- To take overall responsibility for the provision of E-safety
- To ensure the school uses an approved, filtered internet service, which is fully compliant with current statutory requirements
- To be responsible for ensuring that staff receive suitable training to carry out their E-safety roles
- To ensure that robust systems are in place to monitor and support staff who carry out internal E-safety procedures (such as school network manager).

3.2 E-safety Co-ordinator (or Designated Safeguarding Lead if applicable)

- To have day to day responsibility for E-safety issues and to perform a leading role in establishing and reviewing the school E-safety policies
- To promote awareness and commitment to E-safeguarding throughout the school community
- To ensure that all staff are aware of procedures that need to be followed in the event of an E-safety incident (including completion of an incident log)
- To regularly update their own knowledge and understanding of E-safety issues and legislation (and to cascade this to other staff) and remain constantly aware of the potential for serious child protection issues
- To liaise with school ICT technical staff
- To liaise with the local authority and relevant agencies as appropriate.

3.3 Governor

- To ensure that the school follows all authoritative E-safety advice to protect the welfare of students and staff

- To approve the E-safety Policy and regularly review the effectiveness of this policy
- To support the school in encouraging parents and the wider community to become engaged in E-safety activities
- To undertake appropriate training and development on E-safety issues.

3.4 Network Manager/Technician

- To report promptly to the E-safety coordinator any related issues that may arise
- To ensure that users may only access the school's network through an authorised password reinforced by a robust and properly enforced protection policy
- To ensure that provision exists for both detection of misuse and protection against malicious attack (for instance by keeping virus protection up to date)
- To ensure the overall security of the school ICT system
- To ensure that access controls/encryption are in place to protect all personal and/or sensitive information held on school-owned devices.

3.5 Staff

- To be aware of E-safety issues related to the use of mobile phones, cameras and other handheld devices and to monitor their use of such devices to ensure compliance with current school policies
- To report any suspected abuse or breach of policy to the E-safety coordinator
- To maintain an awareness of current E-safety issues, skills development and guidance, for instance through CPD
- To model safe, responsible and professional behaviours in their personal use of information technology.

3.6 Students

- To understand the importance of reporting abuse, misuse or access to inappropriate materials or sites
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To have a good understanding (appropriate to their age and abilities) of research skills and the need to avoid plagiarism and uphold copyright regulations

3.7 Parents/Carers

- To support the school in promoting E-safety
- To consult with the school if they have any concerns about their children's use of technology

4. Education, internet and the curriculum

4.1 The school provides repeated opportunities (within a broad range of curriculum areas) to learn about E-safety and before using the internet students will be made aware of the relevant legislation such as data protection and intellectual property rights.

4.2 Students are also given advice if they experience problems whilst using the internet and/or email and are provided with guidance on promoting E-safety including the requirements to:

- understand the importance of misuse (including accessing inappropriate materials or sites) and are aware of the consequences of this

- understand how to ensure their privacy settings are appropriately configured and to know why they should not post (or share) detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos etc
- understand why they must not post pictures or videos of others without their express consent
- understand issues around plagiarism and how to check copyright etc
- know not to download any files (such as music files) without appropriate permission
- only use approved class email accounts under supervision by (or with permission from) a teacher.

4.3 Each year students are reminded about their responsibilities and details the strategies to maximise learning opportunities whilst reducing potential risks associated with use of the internet.

5. Managing the ICT infrastructure

5.1 In order to effectively manage internet access (including all relevant security issues) the school will:

- block all 'chat rooms' and social networking sites other than those which are part of a recognised educational network or approved learning platform
- only unblock (on a strictly time-limited basis) other external social networking sites for specific purposes/internet literacy lessons
- block access to music download or shopping sites other than those approved for recognised educational purposes at a regional or national level
- use security time-outs on internet access where practicable
- ensure all staff and students have signed an acceptable use agreement form
- Inform all users that internet use is open to continuous monitoring
- make clear that in no circumstances is it acceptable for any individual to log on as another user
- set up the network with shared work areas for (separately) students and staff (students and staff are given appropriate instruction in how to save (and subsequently access) work to (or from) these areas)
- require all users to log off at all times when they have either finished working or are leaving the computer unattended (and in the event that a user finds a computer which is logged on but unattended they are required to always log off and then log on again as themselves).

In the interests of protecting themselves and others, students should bring such instances to the attention of a member of staff in order that suitable instruction may be offered to the previous user.

- set up the network so that users cannot download executable files/programmes
- any ICT software adopted to facilitate the learning of the children or that assists with the provision of education for the children that requires personal information should be subject to a Data Protection Impact Assessment (DPIA) before use. The DPIA should be approved by the Data Protection Officer. The school will only use ICT software providers that are compliant with Data Protection laws.
- make clear that the school's IT department is responsible for ensuring that all equipment that is taken off site has full anti-virus and spyware protection and that this is maintained up-to-date in accordance with school protocols and procedures
- make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities

- ensure that access to the school's network resources from remote locations by staff is restricted to authorised personnel and that access is only through school approved systems.

6. School website

- 6.1 The headteacher has overall responsibility for ensuring that the website content is accurate and that the quality of presentation is maintained in full compliance with the statutory DfE guidelines for publications.
- 6.2 The content of the website will consist primarily of material created by the school itself. Where the content has been published by others (or there are links to such material) the sources will be credited, with a clear statement as to the author's identity or status.
- 6.3 Points of contact detailed on the website are likely to include the school postal address, telephone number and one or more generic email address(es), (such as info@schooladdress or admin@schooladdress). Personal information such as individual e-mail identities will not be disclosed.
- 6.4 Any photographs published on the web will not have full names attached to them and student names will not be recorded when saving images either in the file names or in the tags when publishing on the school website.
- 6.5 Teachers using school approved blogs (or similar) will be expected to ensure that these are password protected and to post contributions from the school website only.

7. Use of ICT equipment at home

- 7.1 Staff and students may be permitted to borrow school ICT equipment for a time-limited period to pursue core school activities at home. Approval for requests must always be granted before equipment is removed from school premises.
- 7.2 Staff should be aware that there are only a limited number of such devices and the school is under no obligation to provide this equipment on demand. If the equipment/computer is used to connect with the internet from the staff member's home, the school will not be responsible for any costs involved.
- 7.3 The school will (as and when resources permit):
- provide a laptop (or other IT equipment) for staff use at home or outside of school
 - ensure that the equipment is working and that repairs are dealt with as quickly and effectively as possible
 - ensure that the computer is covered by insurance for use in and out of school for study purposes, providing reasonable care is taken to prevent loss or damage
 - ensure that the computer is protected against computer viruses and malware
 - maintain and update any software used in school.

8. Use of digital and video photographic images

- 8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have either recorded themselves or have downloaded from the internet.

- 8.2 However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may potentially cause significant harm or embarrassment to individuals in the short or longer term.
- 8.3 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular students should be made aware of the risks attached to publishing their own images on the internet, for instance on social networking sites.
- 8.4 Images taken and used by the school will not be kept for longer than is necessary and will be subject to appropriate security measures.
- 8.5 Staff are allowed to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images, namely that:
- such images should only be taken on school equipment; the personal equipment of staff should not be used for this purpose
 - care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
 - students must not take, use, share, publish or distribute images of others without their express consent
 - photographs taken by students for official school use will be controlled by the school
 - photographs published on the website and other publications (such as newsletters etc) which include students will be selected carefully and will comply with good practice guidance on the use of such images
 - students' full names will not be used anywhere on a website or blog, particularly in association with photographs
 - written permission will be obtained from parents/carers (normally in the form of completion of the appropriate AUP) before photographs of students (or examples of their work) are published on the school website, around school and in school publications.

9. CCTV and monitoring

- 9.1 The school has CCTV on the premises as part of site surveillance for staff and student safety. Recordings (*which are retained by the support provider for 7 days*) will not be revealed without permission except where disclosed to the police as part of a criminal investigation.
- 9.2 Specialist lesson recording equipment is used on occasions as a tool to share best teaching practice. These recordings are only accessible to authorised members of staff and will not be used for any other purposes.

10. Other policies and procedures

- 10.1 This policy will be supported by the following policies and procedures:
- Behaviour Policy (student)
 - Code of Safe Working Practice

- Disciplinary Policy
- Safeguarding Policy
- Social Media Policy