



St. Saviour's Church of England Junior School Staff Acceptable Use of Technology Policy 2023

As a professional organisation with responsibility for safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use of Technology Policy (AUP).

Our Acceptable Use of technology Policy (AUP) is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand St Saviour's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that St Saviour's systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within St Saviour's both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage, online and offline communication technologies.
2. I understand that St Saviour's Acceptable Use of Technology Policy (AUP) should be read and followed in line with St Saviour's Staff Code of Conduct Policy, Child Protection Policy and Online Safety Policy.
3. I am aware that this Acceptable Use of Technology Policy (AUP) is not an exhaustive list and all members of staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School Devices and Systems

4. I understand that any equipment and internet services provided by my workplace are intended for educational use and should only be accessed by members of staff. Personal use of IT school systems / devices by staff is allowed but with the following caveats. The right to personal use can be revoked by the headteacher or governors at any time. Staff use of IT systems / devices must conform to the teacher standards (particularly Part Two: Personal and Professional Conduct). Safeguarding of children is paramount, use of IT by teachers should not place children at risk, violate their privacy or disclose personal details to any non-staff member. Personal information (such as but not limited to personal photographs, videos or any other file which does not relate to the business of the school) should not be stored on school devices; such information or files may be deleted without prior notice.

5. Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
 - I will respect system security and will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
 - I will protect the devices in my care from unapproved access or theft as follows:
 - Never leave my laptop/tablet, camera, mobile telephone unattended in a public place.
 - Keep my home secure against burglars and illicit callers.

- Never leave my laptop/tablet, camera, and mobile telephone on view through windows and glass doors.
 - Never leave my laptop/tablet, camera, and mobile telephone visible in a car.
 - Always password-protect access to my laptop/tablet and mobile telephone.
7. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the Nick Bonell (Headteacher and DSL) or Jez Hoare (SNS).
 8. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the headteacher
 9. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
 - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely.
 - Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school Image/Video Use Policy and will always take into account parental consent (image/video use policy P1).
 - I will not keep documents which contain school-related sensitive or personal information (including digital images, files, videos and emails) on any personal devices, such as laptops, digital cameras or mobile phones.
 10. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
 11. I will not attempt to bypass any filtering and/or security systems put in place by the school. I am aware that the school's internet feed is filtered and protected by RM SafetyNet. I am aware that Nick Bonell and SNS staff (Peter and Jez) carry out separate weekly sweeps of St. Saviour's internet traffic (searches and websites visited) and that any illegal or inappropriate use could result in disciplinary action.
 12. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to Nick Bonell, John Arnold or Jez Hoare as soon as possible.
 13. If I have lost any school related documents or files, I will report this to the Headteacher, DSL (Mr Bonell) as soon as possible.
 14. Any images or videos of pupils will only be used as stated in the school Image and Video Use Policy.
 - I understand images of pupils must always be appropriate and should only be taken with school equipment. They must be taken/published where children's parent/carer have given explicit consent.

Classroom Practice

15. I have read and understood the school's Child Protection Policy which covers the requirements for safe technology use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
 - Exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used in school.
 - Creating a safe environment where children feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
 - Make informed decisions to ensure any online safety resources used with pupils are appropriate.
17. I will report all incidents of concern regarding pupil's online safety to the Headteacher, DSL (Mr Bonell) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Headteacher, DSL (Mr Bonell)

18. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

19. I will ensure that my online reputation and use of information technology and information systems are compatible with my professional role and in line with the Staff Behaviour Policy/Code of Conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
- I will take appropriate steps to protect myself online when using social media
 - I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones
 - I will not discuss, share data or information relating to pupils, staff, school business or parents/carers on social media.
 - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school Code of Conduct/ Acceptable User Policy and the law
20. Electronic communications with current and past pupils, parents/carers and other professionals will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address or telephone number.
 - I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
 - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or parents/carers.
 - If I am approached online by a pupil or parents/carer, I will not respond and will report the communication to my Headteacher, DSL (Mr Bonell).
 - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with my Headteacher, DSL (Mr Bonell).
21. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Headteacher, DSL (Mr Bonell)
22. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
23. I will not create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.
24. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school or the County Council into disrepute.
25. In the event of a Covid-related school closure, I will refer to the school Remote Learning Policy for further guidance

Policy Compliance

26. ***The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use of Technology Policy. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.***

27. Staff are allowed to carry mobile telephones in school. Mobile telephones should, whenever possible be kept out of sight and reach of children, not kept on desks etc. Staff may use their mobile telephone as a watch to check the time but should not be making calls, texts, using social media or internet browsers when there are children present. Any personal mobile telephone use must be in staff areas (staffroom). Mobile telephones should not be logged onto the school wireless network. Staff must not store parent contact information on their personal mobile telephone or use them to take pictures of children (for example at after school/sporting/dance events).

Policy Breaches or Concerns

- 28. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers to the Headteacher, DSL (Mr Bonell) in line with the school’s Child Protection Policy.
- 29. I will report concerns about the welfare, safety or behaviour of staff to the Headteacher, DSL (Mr Bonell)

I have read, understood and agreed to comply with St Saviour’s Church of England Junior School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....