Staff, Governor and Visitor Acceptable Use of I.T. Policy

Person responsible	E-Safety Coordinator & Computing Teacher
Last update	September 2023
Frequency of Review	Annually
Date of next review by Governors	Spring 2024

Why do we have an Acceptable Use Policy (AUP)?

All staff (including support staff), the governing body, visitors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that E-Safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full E-Safety Policy.

What is an AUP?

An AUP outlines how we expect everyone to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). We ask all children, young people and adults involved in the life of St Christopher's to sign one. Children have a specific, tailored AUP to suit their age and learning. All adults are asked to sign the AUP upon first contact with the school and every time changes are made.

This AUP is reviewed annually and linked to our Child Protection Policy, and you will be asked to review and sign it in agreement at the start of each academic year as part of the confirmation of documents or when you join the school during your induction session.. Please note that you will need to be aware of all relevant school level policies.

If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher.

School AUP Agreement?

1. I have read and understood the school Child Protection Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead.
3. I understand the responsibilities for my role in promoting E-Safety. This includes promoting online safety as part of a whole school approach in line with the RSE & PSHE curriculum, as well as safeguarding considerations when supporting pupils in their learning either within the school site or remotely.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

  - not sharing other's images or details without permission
  - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

8. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.

9. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full E-Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL and/or Headteacher.

10. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in the full E-Safety policy.

11. I agree to adhere to all GDPR regulations whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the Headteacher if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

12. I will not store school-related data on personal devices, storage or cloud platforms. USB keys are not to be used. I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

13. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

14. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.

15. I understand and support the commitments made by pupils/students, parents and fellow staff, local committee and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

16. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

17. I understand that breach of this AUP and/or of the E-Safety policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

18. **Should remote learning become necessary:**
    a. **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
    b. **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
    c. **I will not take secret recordings or screenshots** of myself or pupils during live lessons.
    d. **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
    e. **I will maintain the recording of each live session by activating this feature within the Google Classroom meeting.** If anything inappropriate happens or anything which could be construed in this way I shall notify either the DSL or Headteacher as appropriate. This is for my protection as well as that of students
19. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.