Acceptable Use of Technology Policy

This Policy has been approved and adopted by the Xavier Catholic Education Trust in Oct 2022

Committee Responsible: Risk & Audit Committee

To be reviewed in Oct 2023

N.B. This policy is a supplemental policy to the Child Protection and Safeguarding Policy.

Contents

This document should be read in conjunction with other relevant policies including, but not limited to, the Xavier Child Protection and Safeguarding Policy, Online Safety Policy, Behaviour Policy, Relationship and Sex Education Policy, Staff Code of Conduct and Whistleblowing Policy.

Key Stage 3/4/5 Acceptable Use of Technology Policy Agreement

I understand that St John the Baptist School Acceptable Use of Technology Policy will help keep me safe online at home and at school. I understand that I must use school systems in a responsible way.

- I know that technology including school computers, tablets, laptops, and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- I know that my use of school computers and devices, systems and on-site and off-site internet access will be monitored to keep me safe and ensure policy compliance.
- I will keep my password safe and private as my privacy, school work and safety must be protected.
- If I need to learn online at home, I will follow the school remote learning Acceptable Use of Technology Policy.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I will not access social media / messaging apps on my school iPad or during the school day on any device.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.
- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment. I will report any incidents of bullying to an adult.
- I will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos, or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18.
- I will protect my personal information online.
- I will not access or change other people files, accounts, or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I will only use my mobile phone in school if I have permission from a member of staff.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I will always check that any information I use online is reliable and accurate.
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know it can be a criminal offence to gain unauthorised access to systems ('hacking'), make, supply or obtain malware or send threatening and offensive messages.
- I will only change the settings on the computer if a teacher/technician has allowed me to.

- I know that use of the school ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
- I know and understand that if I fail to comply with the Acceptable Use of Technology Policy I will be subject to sanctions. This may include loss of access to the school network/internet, detentions, exclusions, contact with parents/carers and in the event of illegal activities involvement of the police.
- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another pupil which makes me feel worried, scared, or uncomfortable.
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these rules with my parents/carers.

Learners with SEND working significantly below age-related expectations

(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then there will be appropriate sanctions.

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I will tell an adult

Accepting

- I don't open messages from strangers
- I won't open links unless I know they are safe

Reliable

- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online then I don't reply, I save the message and show an adult
- If I see anything online that I don't like, I will tell a teacher or other trusted adult.

Learner Acceptable Use of Technology Policy Agreement

Students sign the AUP on entrance to SJB or via electronic form if there is a significant updates to the policy.

St John the Baptist School Acceptable Use of Technology Policy
Learner Agreement

I have read and understood the *school* Acceptable Use of Technology Policy.

I agree to follow the Acceptable Use of Technology Policy when:

1. I use *school* devices and systems, both on site and at home.
2. I use my own equipment out of the *school*, including communicating with other members of the *school* or when accessing school systems.

Student Name…… Signed…….

Tutor Group…… Date……

Parent/Carer Acknowledgement Form

Parents sign the AUP below electronically on entrance to SJB as part of the enrolment process.

Learner Acceptable Use of Technology Policy: St John the Baptist School Parental Acknowledgment

1. I, with my child, have read and discussed St John the Baptist School learner Acceptable Use of Technology Policy and understand that the Acceptable Use of Technology Policy will help keep my child safe online.

2. I understand that the Acceptable Use of Technology Policy applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.

3. I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

4. I am aware that the school behaviour policy states that my Year 7-11 child cannot use their personal mobile phone on site at any time; it should be switched off and kept securely in their bag/blazer. My Sixth Form child will use their personal mobile phone appropriately, including being discrete and respectful.

5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school Acceptable Use of Technology Policy. When accessing live learning, I will ensure my child is in an appropriate location and that they are suitably dressed.

6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.

7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

8. I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use of Technology Policy or have any concerns about my child's safety online.

9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

11. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name……. Class …….

Parent/Carer's Name…… Parent/Carer's Signature Date……

Staff Acceptable Use of Technology Policy

Staff will sign this policy electronically at the start of their contract period and again if there are significant updates.

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use St John the Baptist School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy.

Our Acceptable Use of Technology Policy 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 Acceptable Use of Technology Policy will help ensure that all staff understand school expectations regarding safe and responsible technology use, and can manage the potential risks posed. The Acceptable Use of Technology Policy will also help to ensure that school 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.

It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy applies to my use of technology systems and services provided to me or accessed as part of my role within St John the Baptist School 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 and online and offline communication technologies**.**

2. I understand that the Acceptable Use of Technology Policy should be read and followed in line with the Xavier Code of Conduct and Child Protection and Safeguarding Policy.

3. I am aware that this Acceptable Use of Technology Policy does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, 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 is intended for educational use and should only be accessed by members of staff.

5. I am aware that the use of the school email for personal use is not permitted.

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 use a 'strong' password to access school systems.
    - I will protect the devices in my care from unapproved access or theft and will on no account leave devices visible or unsupervised in public places.

7. I will respect system security and will not disclose my password or security information to others including IT support staff. If required, I will be provided with a temporary password by IT support staff.

8. 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 IT system manager.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with 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 or accessed remotely.
    - Any data being removed from the school site, such as via email or on a memory stick, will be suitably protected. This may include data being encrypted by a method approved by the school such as in an email typing "ENCRYPT:"

11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved/provided VPN.

12. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

13. 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.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Manager immediately.

16. If I have lost any school related documents or files, I will report this to the ICT Manger and school Data Protection Officer immediately.

17. I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

18. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning and other working spaces, including appropriate supervision of learners, as outlined in the school Online Safety Policy and Child Protection and Safeguarding Policy.
19. I have read and understood the school online safety policy which covers expectations for learners regarding mobile technology and social media.
20. I will promote online safety with the learners 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 on site.
    - creating a safe environment where learners 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.
    - involving the Designated Safeguarding Lead or Deputy Safeguarding Lead as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.

- make informed decisions to ensure any online safety resources used with learners is appropriate.

21. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL and IT Manager in line with the School online safety and child protection and safeguarding policy.
22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and 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

23. I have read and understood the School Online Safety Policy which covers expectations regarding staff use of mobile technology and social media.
24. I will ensure that my online reputation and use of IT and information systems is compatible with my professional role and in line with the Code of Conduct, Online Safety Policy and Child Protection and Safeguarding Policy and the law 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 as outlined in the Online Safety Policy.
    - I am aware of school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the Online Safety Policy.
    - I will not discuss or share data or information relating to learners, 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 Code of Conduct and the law.

25. My electronic communications with current and past learners and parents/carers 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 learners, 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 learners and/or their parents/carers.
    - If I am approached online by a current learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).

- Any pre-existing relationships or situations that compromise my ability to comply with the Acceptable Use of Technology Policy will be discussed with the Headteacher.

26. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Headteacher.

27. 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.

28. I will not attempt to access, 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.

29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Policy Compliance

30. I understand that St John the Baptist School may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

31. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school Child Protection and Safeguarding Policy.

32. I will report and record concerns about the welfare, safety or behaviour of staff to the Headteacher in line with the Child Protection and Safeguarding Policy and Staff Code of Conduct.

33. I will report and record concerns about the welfare, safety or behaviour of the Headteacher to the Xavier CEO, Ani Magill.

34. I understand that if St John the Baptist School believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the Code of Conduct.

35. I understand that if St John the Baptist School believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the Code of Conduct.

36. I understand that if St John the Baptist School suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with the 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)……..

Visitor and Volunteer Acceptable Use of Technology Policy

Any visitors accessing any school IT systems (wifi / network etc.) are made aware of the AUP policy and in logging on they are agreeing to it and signing it electronically.

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology.

This Acceptable Use of Technology Policy will help St John the Baptist School ensure that all visitors and volunteers understand the school expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy applies to my use of technology systems and services provided to me or accessed as part of my role within St John the Baptist School 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, remote learning systems and communication technologies.

2. I understand that this Acceptable Use of Technology Policy should be read and followed in line with the School Staff Code of Conduct.

3. I am aware that this Acceptable Use of Technology Policy does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, Xavier Code of Conduct and the School Child Protection and Safeguarding policy, national and local education and child protection guidance, and the law.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am not allowed to take images or videos of learners unless given express permission by the Headteacher.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the School Online Safety Policy**.**

7. Where I deliver or support remote learning, I will comply with the school remote learning Acceptable Use of Technology Policy.

8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) in line with the School Child Protection and Safeguarding Policy.

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

Use of Social Media and Mobile Technology

11. I have read and understood the School Online Safety Policy which covers expectations regarding use of social media and mobile technology.

12. I will ensure that my online reputation and use of technology is compatible with my role within St John the Baptist School. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the Online Safety Policy
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the School Staff Code of Conduct and the law.

13. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL and/or headteacher.

Policy Compliance, Breaches or Concerns

14. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead and/or the headteacher.

15. 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.

16. I will not attempt to access, 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.

17. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

18. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors or volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

19. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the School Child Protection and Safeguarding Policy and Code of Conduct.

20. I will report concerns about the welfare, safety, or behaviour of staff to the Headteacher, in line with the School Child Protection and Safeguarding Policy and Code of Conduct.

21. I will report concerns about the welfare, safety or behaviour of the Headteacher to the Xavier CEO Ani Magill.

22. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

23. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St John the Baptist School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ……

Signed: ……

Date (DDMMYY)……..

Wi-Fi Acceptable Use Policy (Can be electronic)

Any users accessing the school wifi network are required to subscribe to the below AUP, signing it electronically on login.

As a professional organisation with responsibility for children's safeguarding it is important that all members of St John the Baptist School community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.
This is not an exhaustive list and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. St John the Baptist School provides Wi-Fi for the school community and allows access for school business and education use only.

2. I am aware that St John the Baptist School will not be liable for any damages or claims of any kind arising from the use of the Wi-Fi. St John the Baptist School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under St John the Baptist School Acceptable Use of Technology Policy, Online Safety Policy, Behaviour Policy, Code of Conduct, Child Protection and Safeguarding Policy and Data Protection Policy which all learners/staff/visitors and volunteers must agree to and comply with.

4. St John the Baptist School reserves the right to limit the bandwidth of the Wi-Fi, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. St John the Baptist School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school Wi-Fi is not secure and the school cannot guarantee the safety of traffic across it. Use of the school Wi-Fi is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any Wi-Fi network. I confirm that I knowingly assume such risk.

8. St John the Baptist School accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school Wi-Fi connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other

internet-borne programs is my sole responsibility; and I indemnify and hold harmless St John the Baptist School from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the St John the Baptist School security and filtering systems or download any unauthorised software or applications.

11. My use of St John the Baptist School Wi-Fi will be safe and responsible and will always be in accordance with the Acceptable Use of Technology Policy and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring St John the Baptist School into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the headteacher.

15. I understand that my use of the St John the Baptist School Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then St John the Baptist School may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.