



Technology & Online Safety User Requirements

Users accessing any technology or online system provided by one of Xavier's schools is required to abide by the following statements

Publication Date: Updated September 2026

Review Date: July 2027

Reviewer: Anna Dwyer

Executive Statement

Safeguarding, Technology and Data Protection

At Xavier Catholic Education Trust, safeguarding is at the heart of everything we do. We take our responsibility to protect children, young people, staff and the wider school community extremely seriously. In today's digital world, safeguarding extends beyond physical environments and includes the safe, ethical and secure use of technology, data and artificial intelligence.

The Trust is committed to ensuring that all personal information entrusted to us is handled lawfully, securely and responsibly. Protecting the confidentiality, integrity and availability of data is a key part of our safeguarding responsibilities. We work closely with our Trust Data Protection Officer (DPO) to evaluate risks, ensure compliance with data protection legislation and continuously review our practices to maintain high standards of information security.

We make carefully considered decisions about the technology, software, online services and artificial intelligence tools used across our schools. Before introducing new systems, the Trust undertakes appropriate due diligence, including assessments of safeguarding, security, privacy, educational value and legal compliance. This helps us ensure that the technology we use supports learning while protecting those who depend upon it.

We recognise that technology is evolving rapidly, particularly in relation to Artificial Intelligence (AI). When referring to AI, we do not mean only generative AI tools such as ChatGPT, Microsoft Copilot or image generators. AI encompasses a wide range of technologies, many of which are already embedded within educational software and digital services used every day. These technologies may be used to personalise learning experiences, provide feedback, improve accessibility, strengthen cyber security, support safeguarding, analyse data and enhance operational efficiency. As AI continues to develop, the Trust remains committed to ensuring that its use is educationally beneficial, ethically sound, secure and appropriately managed. To ensure our staff remain informed and confident in this changing landscape, all employees receive annual training on safeguarding, data protection and cyber security. In addition, colleagues are supported to develop their understanding of emerging technologies, including AI, so that they can make informed decisions and model safe, responsible practice for our learners.

Equipping children and young people with the knowledge and skills to navigate the digital world safely is an essential part of our educational mission. Across our schools, students receive a high-quality curriculum that develops their understanding of online safety, social media, digital citizenship, data protection and artificial intelligence. We aim to empower young people to recognise and manage risks, think critically about online content and make safe, informed choices when using technology.

An important aspect of this education is helping children and young people understand consent and respect in digital environments. Learners are taught what consent means in relation to sharing information, images, videos and personal data, as well as the responsibilities that accompany the use of technology. By promoting understanding, respect and accountability, we seek to create a culture where technology is used safely, ethically and for the benefit of all.

These Technology and Online Safety User Requirements form part of that commitment and help ensure that everyone within our Trust community understands their role in maintaining a safe, secure and respectful digital environment.

Contents

Please read the sections relevant to your role and/or the age of your child or the children you work with.

1.	KS3, KS4 and KS5 Students.....	4
2.	KS2 Students.....	9
3.	Reception and KS1 Students	14
4.	Students with SEND	17
5.	Parents and carers.....	19
6.	Staff, Governors, Volunteers and Visitors.....	23
	Appendix A: Technology, Online Safety and Artificial Intelligence Glossary	26
	Appendix B: Photograph and video consent wording and descriptions.....	29

Linked Policies

This document should be read in conjunction with the following Xavier Policies that can be accessed via our website:

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Online Safety Policy
- AI Policy
- Behaviour Policy (individual school websites)
- Trust Privacy Notices

1. KS3, KS4 and KS5 Students

By logging on to a school device or technology system (including but not limited to email, Windows PCs, iPads, Chrome Books etc.) students are expected to follow the learner requirements detailed below.

Students will be walked through this periodically as part of their PSHE and/or Computing curriculum to ensure that they understand their responsibilities.

Where the school identifies students with SEND who are working below age expectations, they will be provided with scaffolding to ensure that they can access the key points and understand what they are agreeing to; this may include use of the KS2, KS1 or SEND learner requirements as appropriate.

KS3, KS4 and KS5 Learner Technology & Online Safety Requirements

(Including Artificial Intelligence and Data Consent)

This explains how I am expected to use technology, online services, and Artificial Intelligence (AI) as a learner at this school. These rules help keep me safe, protect others, and make sure technology is used for learning.

This applies **in school, at home, and anywhere I am using school accounts, systems, devices, or learning platforms.**

I understand that I am responsible for how I use technology and will take this responsibility seriously.

1. Using School Technology Safely

I agree that I will:

- Use school computers, devices, networks, email, Teams, online platforms, and learning apps for learning and school-related purposes only
- Keep my username and password private and not share them with anyone
- Log out of shared devices and lock screens when asked
- Look after school equipment and report damage, loss, or technical problems promptly
- Only use software, websites, apps, and AI tools approved by the school

I understand that trying to hack, bypass filters, access blocked content, or interfere with systems is not allowed and will be sanctioned in line with the school behaviour policy.

2. Respectful and Responsible Behaviour Online

I agree that I will always be respectful online, just as I am expected to be in school.

I will not:

- Bully, harass, threaten, impersonate, or intimidate anyone
- Use hateful, extremist, racist, sexist, misogynistic or offensive language

- Share false or misleading information
- Damage the reputation of the school or others
- Encourage others to break these rules on my behalf

I understand that online behaviour outside school may still be dealt with by the school if it affects safety, wellbeing, or the school community.

These rules do not stop me telling a trusted adult about something that worries me, including something involving the school.

3. Images, Videos, and Sharing Content

I understand that:

- I must never create, upload, share, request, or forward nude or semi-nude images, videos, livestreams, or AI-generated images of this type. This includes "jokes", memes, dares, private messages, "sexting" or content shared with consent.
- If you are under 18, it is against the law to:
 - take, possess or send nude or semi-nude photos, including selfies
 - possess or share indecent images of someone under 18, including images generated by AI
 - encourage or incite someone to take or send 'sexts' or 'nudes'
 - take a photo of your own genitals, whether the image is shared on or not

This is the case even if you are sharing it with someone you are in a relationship with.

- The law considers any taking, making, or sharing of nude or semi-nude images involving anyone under the age of 18 as a form of child abuse whether it is consent is given or not.

I understand that the school may need to involve parents, carers, safeguarding staff or other agencies (in extreme cases this may have to involve the police) if there is a serious safety concern.

I will tell a trusted adult straight away if anyone sends me this type of image or asks me to share one. I will tell a trusted adult and will not forward it.

I will not:

- Share any images or videos of others without permission
- Share school or personal information about others online

I will not be in trouble simply for receiving an unwanted image or asking for help.

4. Artificial Intelligence (AI) Use

AI can support learning when used properly and with integrity. I agree that I will:

- Only use school-approved AI tools, in ways explained by my teacher
- Use AI to support learning, not to replace my own thinking
- Never present AI-generated work as my own
- Clearly acknowledge AI use when required
- Follow teacher instructions about AI use in homework, coursework, assessments, and exams

I will not:

- Use AI to cheat, plagiarise, or avoid learning
- Use AI to create harmful, misleading, offensive, or inappropriate content
- Enter personal, sensitive, or identifiable data into AI tools unless the school has approved it as secure

I understand that misuse of AI will have a negative impact on my learning and could lead to sanctions.

5. Personal Data and Online Accounts

I understand that:

- The school must process my data safely and lawfully
- My activity on school systems may be monitored and logged for safety, safeguarding, and security
- Filters are used to protect users but are not perfect

I agree that I will:

- Think carefully before signing up for online accounts
- Respect age restrictions on websites and apps
- Protect my personal information and the information of others

6. Monitoring and Sanctions

I understand that the school:

- Monitors internet use, school accounts, and devices for safeguarding and security purposes
- May investigate concerns involving technology or online behaviour
- Can apply sanctions if I misuse technology, even outside school, where appropriate

Sanctions will follow the school's behaviour and safeguarding procedures.

7. Reporting and Support

I agree that I will:

- Tell a trusted adult if something online or in an AI tool worries me
- Report unsafe content, messages, or behaviour
- Be an upstander, not a bystander

If I need help, I can also use:

- www.thinkuknow.co.uk
- www.childnet.com
- www.childline.org.uk

8. Consent

I understand that:

- The school needs to use some information about me to provide education and keep me safe
- My parent or carer usually decides whether the school can use photographs or videos of me for publicity and communication purposes.

Photos and videos may be used:

- During school activities for education, care and safety
- In school displays, newsletters and learning materials
- On the school website, prospectus and other publicity materials
- On official school or Trust social media accounts

My parent or carer can change their decision at any time by contacting the school (details of these consents can be found in appendix B)

I understand that:

- The school may use approved AI-enabled educational technologies to support my education and learning, at times this may include uploading work and/or personal data.

Declaration

I confirm that:

- I have read and understood these requirements
- I understand that sanctions may apply if I misuse technology
- I agree to follow these rules whenever I use school technology or online service.

In addition, please read the section that applies to you.

A. Learners Under 13 Years Old

I understand that my parent/carer may be asked to provide consent for the use of my photographs or videos where consent is required. I will talk with them about this so that they can consider my wishes.

B. Learners Aged 13 and Over

I have rights over my personal information whatever my age. The school will involve me in decisions about photographs and videos in a way that reflects my age, understanding and maturity.

Photography and video consent preferences are normally recorded through a parent/carer consent process. I should talk to my parent/carer about my wishes and feelings regarding the use of my image.

If I have concerns about how my photograph or video is being used, I should speak to a parent/carer or a member of school staff.

By logging on to a school device or technology system I am agreeing to follow the Technology and Online Safety User Requirements.

2. KS2 Students

By logging on to a school device or technology system (including but not limited to email, Windows PCs, iPads, Chrome Books etc.) students are expected to follow the learner requirements detailed below.

Students will be walked through this periodically as part of their PSHE and/or Computing curriculum to ensure that they understand their responsibilities.

Where the school identifies students with SEND who are working below age expectations, they will be provided with scaffolding to ensure that they can access the key points and understand what they are agreeing to; this may include use of the KS1 or SEND learner requirements as appropriate.

KS2 Learner Technology & Online Safety Requirements

This explains how I should use technology, online services and Artificial Intelligence (AI) at school.

These rules help to keep me safe, help me learn, and help me be kind and respectful to others.

These rules apply at school, at home, and anywhere I use school devices, accounts, systems or learning apps.

I understand that I am responsible for how I use technology and will take this responsibility seriously.

1. Using School Technology Safely

I agree that I will:

- Use school computers, devices, the internet, email, Teams and learning apps for schoolwork and learning
- Keep my username and password private
- Log out when I finish using a shared device if I am asked to
- Look after school equipment and tell an adult if something is broken, lost or not working properly
- Only use websites, apps and AI tools that my school or teacher says I can use

I understand that I must not try to get around school internet filters, access blocked websites, or interfere with school systems.

2. Respectful and Responsible Behaviour Online

I agree that I will be kind and respectful online, just as I am in school.

I will not:

- Be unkind, bully, threaten or upset anyone online
- Pretend to be someone else
- Use rude, offensive or hurtful language
- Share things that I know are not true
- Say or do things that could harm the reputation of the school or another person

- Ask other people to break these rules for me

I understand that the school may need to deal with online behaviour outside school if it affects the safety or wellbeing of others.

These rules do not stop me telling a trusted adult about something that worries me, including something involving the school.

3. Images, Videos, and Sharing Content

I understand that:

- I must never create, ask for, send, share or save pictures or videos showing private body parts
- I must tell a trusted adult straight away if anyone sends me this type of image or asks me to share one
- Sharing these images of children is against the law and will always be treated seriously

I will not:

- Share photos or videos of other people without their permission
- Share personal information about myself or other people online

I will not be in trouble simply for receiving an unwanted image or asking for help. I will tell a trusted adult and will not forward it.

I understand that the school may need to involve parents, carers, safeguarding staff or other agencies if there is a serious safety concern.

4. Artificial Intelligence (AI) Use

AI can help me learn when it is used properly.

I agree that I will:

- Only use AI tools that my teacher or school has approved
- Use AI to help me learn rather than do my work for me
- Complete my own work and show my own understanding
- Tell my teacher if I have used AI when asked to
- Follow my teacher's instructions about using AI in lessons and homework
- My teacher will tell me which tools and features I may use. I must not use generative AI chatbots, such as ChatGPT, directly for school activities unless specifically instructed by my teacher.
- If I see an AI feature that I have not been told to use, I will ask my teacher first.

I will not:

- Use AI to cheat

- Copy AI work and pretend it is my own
- Use AI to create unkind, harmful or inappropriate content
- Type personal information into AI tools unless my school says it is safe to do so

I understand that using AI in the wrong way may lead to consequences and affect my learning.

5. Personal Data and Online Accounts

I understand that:

- The school keeps information about me safe and uses it to help run the school
- My use of school devices and accounts may be checked to help keep everyone safe
- Internet filters help protect me online, but they do not block everything

I agree that I will:

- Think carefully before creating online accounts
- Follow the age rules for websites and apps
- Keep my personal information safe
- Respect the personal information of other people

6. Monitoring and Sanctions

I understand that the school:

- Checks internet use, school accounts and devices to help keep everyone safe
- May investigate concerns about technology use or online behaviour
- May apply consequences if I misuse technology, including when this affects the school community outside school

Any consequences will follow the school's behaviour and safeguarding policies.

7. Reporting and Support

I agree that I will:

- Tell a trusted adult if something online worries, upsets or confuses me
- Tell a trusted adult if I receive or am asked to send messages that are unkind or contain pictures or videos that worry, upset or confuse me
- Report unsafe messages, websites or behaviour
- Help others by speaking up if someone needs support

If I need help, I can also use:

- www.thinkuknow.co.uk
- www.childnet.com
- www.childline.org.uk

8. Consent

I understand that:

- The school needs to use some information about me to provide education and keep me safe
- My parent or carer usually decides whether the school can use photographs or videos of me for publicity and communication purposes.

Photos and videos may be used:

- During school activities for education, care and safety
- In school displays, newsletters and learning materials
- On the school website, prospectus and other publicity materials
- On internal school communication channels

The school will not publish identifiable images of any primary school children on social media.

My parent or carer can change their decision at any time by contacting the school (details of these consents can be found in appendix B).

I understand that:

- The school may use approved AI-enabled educational technologies to support my education and learning, at times this may include uploading work and/or personal data.

Declaration

I confirm that:

- I have read and understood these requirements.
- I understand that sanctions may apply if I misuse technology
- I agree to follow these rules whenever I use school technology or online service.

In addition, please read the section that applies to you.

I understand that my parent or carer makes decisions about consent for my personal information, photographs and videos. I can talk to them about my wishes and feelings.

By logging on to a school device or technology system I am agreeing to follow this Technology and Online Safety User Requirements.

--

3. Reception and KS1 Students

By logging on to a school device or technology system (including but not limited to email, Windows PCs, iPads, Chrome Books etc.) students are expected to follow the learner requirements detailed below.

Students will be walked through this periodically as part of their PSHE and/or Computing curriculum to ensure that they understand their responsibilities.

Where the school identifies students with SEND who are working below age expectations, they will be provided with scaffolding to ensure that they can access the key points and understand what they are agreeing to; this may include use of the SEND learner requirements as appropriate.

Reception and KS1 Learner Technology & Online Safety Requirements

This explains how I should use computers, tablets, the internet and AI at school.

These rules help to keep me safe, help me learn and help me be kind to other people.

These rules apply at school, at home and anywhere I use school technology.

I promise to do my best to follow these rules.

1. Keeping Myself Safe

I will:

- Only use websites, apps and AI tools that my teacher or parent/carer says I can use
- Keep my password secret
- Tell an adult if something online worries, upsets or confuses me
- Look after school computers and devices
- Tell an adult if a device is broken or not working

I will not:

- Click on things that I am not sure about
- Try to get onto websites that my teacher has not allowed
- Share my personal information online
- Send, ask for, save or share pictures of private body parts

If someone sends me something that worries or upsets me, I will tell a trusted adult straight away.

2. My Learning

I will:

- Use school technology to help me learn
- Listen to my teacher and follow instructions
- Use AI to help me learn when my teacher says it is okay
- Do my own work and try my best

I will not:

- Let AI do all my work for me
- Copy work from AI or other people and say it is my own

3. My Responsibility

I will:

- Be kind and respectful online
- Use kind words and good manners
- Be honest online
- Keep other people's information safe
- Ask permission before sharing photos or videos of other people

I will not:

- Be unkind or bully anyone online
- Pretend to be someone else
- Send rude or hurtful messages
- Share things that I know are not true

I understand that the school helps to keep everyone safe by checking how school technology is used.

4. Getting Help

If something online worries, upsets or confuses me, I will:

 Stop

 Turn off the screen or put the device down

 Tell a trusted adult

I will also tell an adult if:

- Someone is being unkind online
- I see something unsafe
- Someone asks me to keep an online secret
- Someone asks me to send a picture or message that makes me feel uncomfortable

I will try to help others by speaking up when they need help.

5. Agreement

I understand that:

- The school uses information about me to help me learn and stay safe
- My parent or carer decides whether the school can use photographs or videos of me
- There may be consequences if I do not follow these rules

6. My Promise

I promise that I will:

- Use technology safely
- Be kind and respectful
- Tell an adult if I need help
- Follow these rules whenever I use school technology

My parent or carer helps make decisions about my personal information, photographs and videos, and I can talk to them about how I feel.

By logging on to a school device or technology system I am agreeing to follow this Technology and Online Safety User Requirements.

4. Students with SEND

By logging on to a school device or technology system (including but not limited to email, Windows PCs, iPads, Chrome Books etc.) students are expected to follow the learner requirements detailed below.

Students will be walked through this periodically as part of their PSHE and/or Computing curriculum to ensure that they understand their responsibilities.

Where the school identifies students with SEND who are working below age expectations, they will be provided with scaffolding to ensure that they can access the key points and understand what they are agreeing to.

SEND Learner Technology & Online Safety Requirements

These rules help me stay safe, be kind and learn.

1. Keeping Myself Safe

I will:

- ☒ Tell an adult if something worries me
- ☒ Use websites and apps my teacher says I can use
- ☒ Keep my password secret
- ☒ Look after school computers and tablets

I will not:

- ☒ Share my name, address or other personal information online
- ☒ Send or share pictures of private body parts
- ☒ Use websites my teacher has not said I can use

2. My Learning

I will:

- ☒ Use computers and tablets for learning
- ☒ Listen to my teacher
- ☒ Try my best
- ☒ Do my own work

I can use AI when my teacher says it is okay.

3. My Responsibility

I will:

- ☒ Be kind to other people
- ☒ Use kind words online
- ☒ Tell the truth
- ☒ Ask before sharing photos of other people

I will not:

-  Be mean to other people
-  Say unkind things online
-  Pretend to be someone else

4. Getting Help

If something online makes me worried, upset or confused, I will:

-  Stop
-  Turn off the screen or put the device down
-  Tell a trusted adult

I will tell an adult if:

- Someone is being unkind
- I see something scary or upsetting
- Someone asks me to keep an online secret
- Someone asks me to send a picture or message

5. My Promise

I promise to:

-  Be safe
-  Be kind
-  Use technology for learning
-  Ask for help when I need it
-  Follow these rules when I use school technology

When I log on to a school computer, tablet or app, I am agreeing to follow these rules.

5. Parents and carers

Parents and Carers who choose to send their child to a Xavier CET School are agreeing to abide by these requirements and to support their child in understanding their responsibilities.

Parent/Carer Technology & Online Safety Requirements

Technology plays an important role in teaching, learning, communication and safeguarding across the Trust. Learners use a range of digital systems, devices and online services to access the curriculum, complete learning activities, communicate with staff and develop their digital skills.

The use of school technology systems is a normal and necessary part of a learner's education. These systems help the school deliver education, safeguard learners and fulfil its statutory responsibilities.

This explains how we work in partnership with parents and carers to promote safe, responsible and effective use of technology.

1. Communication with the School

The school uses a range of official communication channels, including:

- The school website
- Email
- Arbor
- Microsoft Teams and other learning platforms
- Official school social media accounts
- Text messaging and notification services

When communicating with the school, I will:

- Be respectful towards staff, learners and other parents/carers
- Communicate in a courteous and constructive manner
- Raise concerns through the school's official procedures so they can be investigated and resolved appropriately
- Respect the privacy and wellbeing of members of the school community

I will not:

- Use social media, messaging groups or online forums to criticise, harass or make personal comments about members of staff
- Use social media or messaging groups to discuss, investigate or attempt to resolve incidents involving other children
- Share confidential or sensitive information relating to the school community
- Upload or share photographs or videos containing other children without appropriate permission
- Send excessive, repetitive or unreasonable volumes of correspondence that hinder the school's ability to respond effectively. If I have an issue that I would like to raise, I will use the school's normal communication channels so that it can be considered and addressed appropriately.

These requirements do not prevent parents and carers from raising concerns or seeking advice. Parents and carers remain responsible for communicating respectfully.

2. Supporting Safe & Effective Use of Technology

I understand that:

- My child will use school technology systems, devices, online learning platforms and digital resources as part of their education.
- Access to these systems is an important and necessary part of the school's educational provision and curriculum delivery.
- The Learner Technology and Online Safety Requirements apply whenever my child uses school systems, accounts, devices or learning platforms, whether at school or at home.
- The school monitors the use of its systems and devices for safeguarding, security and operational purposes.
- Internet filtering and monitoring systems help to protect learners but cannot eliminate all online risks.
- Artificial Intelligence (AI) tools may be used within the curriculum where approved by the Trust and supported by appropriate safeguards.
- The school may apply appropriate behaviour, safeguarding or disciplinary measures where technology is misused.
- If I have questions, concerns or require further information about the digital systems used by the school, I should contact the school directly.

I will:

- Read and discuss the relevant Learner Technology and Online Safety Requirements with my child.
- Encourage safe, respectful and responsible behaviour online.
- Support the school's online safety policies and procedures.
- Ensure that access to the internet outside school is appropriately supervised according to my child's age, maturity and needs.
- Use parental controls and other appropriate online safety measures where available including on any mobile devices my child has access to.
- Work in partnership with the school to support my child's safe and effective use of technology.

3. Photographs, Videos and Consent

I understand that the school requires specific parental consent before using photographs or video recordings of my child for purposes beyond those necessary for education, pastoral care, safety and security.

Consent preferences for photographs and videos are managed through Arbor and include:

- Internal school displays, newsletters and learning materials
- School and Trust websites, prospectuses and promotional materials
- Official school or Trust social media channels
- Other approved publicity and communication activities

It is important to note that Xavier CET Schools will not publish identifiable images of primary age children on social media channels. Secondary schools will ask explicitly for parental consent to publish identifiable photos of children on social media.

The Trust records photography and video consent preferences through a parent/carer consent process. The school will also take account of the views and wishes of children and young people where appropriate.

I understand that:

- Photograph and video consent is separate from my child's use of school technology systems
- I can review my photograph and video consent preferences at any time through Arbor. To amend them once given/declined in Arbor I must email the school directly.
- The school will respect the preferences I have recorded
- The school may use approved AI-enabled educational technologies to support my child's education and learning. Where student work or personal data is processed, this will be done securely and in accordance with the Xavier AI Policy and relevant data protection requirements.
- Staff and students may use only the tools and features approved by the Trust for their particular purpose and age group.
- Where a Data Protection Impact Assessment (DPIA) is required, the relevant processing will not start or restart until the assessment is complete, and the necessary safeguards are in place.
- Any use currently subject to a pause will remain paused until the Trust has approved its resumption following completion of the required assessments and safeguards.
- Acceptance of these requirements does not alter or override any such restrictions or pauses.

Information about approved AI uses, safeguards and any restrictions that apply within the school will be communicated to parents and carers through the school's normal communication channels.

Significant changes to how AI technologies are used with students will be communicated before implementation where appropriate.

Full details of the photograph and video consents can be found in appendix B.

Declaration

I confirm that:

- I have read and understood these requirements.
- I understand that the use of school technology systems is an important part of my child's education
- I have read, or will read, the relevant Learner Technology and Online Safety Requirements with my child
- I will support the school in promoting safe, responsible and effective use of technology
- I will contact the school if I have any questions or concerns regarding technology use, online safety, AI or digital learning

For clarity, following these requirements, logging into a school account, using school technology systems or remaining enrolled at the school does not constitute consent to personal data processing. Where the school relies on consent, it will be requested separately and specifically. Processing carried out under other lawful bases is explained in the Trust's Privacy Notices.

By remaining enrolled at the school, learners will be provided with access to the technology systems and digital services necessary to support their education, subject to compliance with the school's policies and procedures.

6. Staff, Governors, Volunteers and Visitors

Access to school and Trust technology systems is provided to support education, administration, governance, safeguarding and operational activities.

By logging on to, accessing, or using any school or Trust device, network, account, application, or online service, users understand and agree to follow the below requirements.

Staff, Governors, Volunteers and Visitors Technology & Online Safety Requirements

1. General Responsibilities

- I understand that these requirements apply whenever I use school or Trust technology systems, devices, accounts, networks or online services.
- I will act professionally and responsibly when using technology and digital communication tools.
- I will follow these requirements alongside the Xavier Code of Conduct, Child Protection and Safeguarding Policy, Online Safety Policy, Data Protection Policy, AI Policy and other relevant policies.
- I understand that not every possible situation can be covered in these requirements and that I must always act in accordance with safeguarding requirements, professional standards and the law.

2. Use of School Devices and Systems

- I will use school and Trust technology systems primarily for school, Trust or governance-related purposes.
- I will only access systems, devices and information that I am authorised to use.
- I will use school email and communication systems professionally and appropriately.
- I will take reasonable care of any devices or equipment provided to me.
- I understand that access to school systems is provided to support my role and may be withdrawn if it is misused.

3. Data and System Security

- I will keep passwords secure and will not share them with anyone.
- I will lock or log out of devices when they are unattended.
- I will handle personal and sensitive data in accordance with UK GDPR, data protection legislation and school policies.
- I will not store school-related sensitive information on personal devices unless specifically authorised and protected by approved security measures.
- I will not install unauthorised software, applications or hardware.
- I will not attempt to bypass security controls, monitoring systems or internet filtering.
- I will report suspected phishing emails, malware, security weaknesses or cyber security incidents promptly.
- I will report the loss of any device, document or data containing school information immediately.
- I will only use AI tools approved by the Trust or school when processing school information.

- I will not enter personal, confidential or student data into AI systems unless they have been approved for that purpose and appropriate safeguards are in place.
- I will only use learner images and videos in accordance with school policies and recorded consent preferences. (Full details of the photograph and video consents can be found in appendix B).
- Before publishing or sharing an image for a purpose that relies on consent, I will check the current permissions for identifiable students featured. If permission is absent or unclear, I will select another image, crop or obscure identity, or not use it.

4. Classroom Practice

(Applicable where individuals work directly with learners)

- I will model safe, responsible and appropriate use of technology.
- I will support learners to develop safe and responsible online behaviours including the use of AI.
- I will supervise learner use of technology appropriately.
- I will create an environment where learners feel confident reporting online safety concerns.
- I will report any safeguarding concerns, inappropriate content, filtering breaches or online safety incidents in line with school procedures.
- I will respect copyright, intellectual property and licensing requirements.
- I will use AI responsibly, transparently and in accordance with the Xavier AI Policy.
- I will ensure students only use AI tools and features approved by the Trust.

5. Social Media and Mobile Technology

- I will maintain professional boundaries at all times when communicating online.
- I will use approved school communication systems when communicating with learners, parents or carers.
- I will not share personal contact details with learners.
- I will not add or accept learners as contacts on personal social media accounts.
- I will not share confidential or sensitive information relating to learners, staff, parents, governors or the Trust through social media or personal communication channels.
- I will ensure my online behaviour does not undermine my professional role or bring the school or Trust into disrepute.
- I will seek advice from the Headteacher, DSL or IT team if I am unsure about appropriate online practice.
- I will ensure that photographs and videos of children are taken and used in accordance with school procedures and recorded consent preferences.
- I will not post identifiable images of primary age children on social media.

6. Content and Behaviour

- I will use technology in a lawful, professional and appropriate manner.

- I will not access, create, store, transmit or share illegal, harmful, offensive, discriminatory or inappropriate content.
- I will not engage in online behaviour that could compromise safeguarding, professional standards or the reputation of the school or Trust.
- I will treat others with respect and professionalism in all digital communications.

7. Policy Compliance and Reporting

- I understand that the school and Trust monitor the use of devices, networks, systems and accounts for safeguarding, security and operational purposes.
- I will report concerns relating to learner welfare or online safety to the Designated Safeguarding Lead (DSL).
- I will report data breaches, information security incidents or lost data immediately in accordance with school procedures.
- I will report concerns about staff conduct to the Headteacher.
- I will report concerns about the Headteacher to the Xavier CEO.
- I understand that breaches of these requirements may result in disciplinary action, removal of access rights, referral to relevant professional bodies, or referral to external agencies where appropriate.
- I understand that suspected criminal activity may be reported to the police.

By logging on to a school device or technology system I am agreeing to follow this Technology and Online Safety User Requirements.

Appendix A: Technology, Online Safety and Artificial Intelligence Glossary

This glossary explains some of the terms used throughout this document. The definitions are intended to support understanding and are not legal definitions.

Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to computer systems that can perform tasks which would normally require human intelligence, such as generating text, creating images, answering questions, analysing information or making predictions.

Generative AI

Generative AI is a type of AI that creates new content, such as text, images, audio, video or computer code, based on information it has learned from large amounts of data.

Large Language Model (LLM)

A Large Language Model (LLM) is a type of AI system trained on vast amounts of text. LLMs can generate human-like language, answer questions, summarise information and assist with writing tasks. Examples include Microsoft Copilot, ChatGPT and Google Gemini.

AI Tool

An AI tool is any software, application or online service that uses Artificial Intelligence to perform tasks, assist users or generate content.

Machine Learning

Machine Learning is a branch of AI that enables computers to learn from data and improve their performance without being explicitly programmed for every task.

Personal Data

Personal data is any information that can identify an individual directly or indirectly. Examples include names, photographs, email addresses, student numbers, dates of birth and online identifiers.

Special Category Data

Special category data is particularly sensitive personal information that requires additional protection. Examples include information relating to health, ethnicity, religion or biometric information.

Data Protection

Data protection refers to the rules, practices and safeguards used to ensure personal information is handled lawfully, fairly, securely and transparently.

Consent

Consent means giving a clear and informed agreement for something to happen. In a technology context, this may include agreeing to the use of personal information, photographs, videos or online services. Consent should be freely given and may be withdrawn where appropriate.

Digital Footprint

A digital footprint is the record of information created when someone uses the internet or digital technology. This may include websites visited, social media activity, messages, photographs and online accounts.

Online Safety

Online safety refers to the actions taken to protect people from harm when using technology, the internet, social media, gaming platforms or other digital services.

Cyber Security

Cyber security is the protection of devices, networks, systems and data from unauthorised access, attack, damage or loss.

Data Breach

A data breach occurs when personal or confidential information is accidentally or unlawfully lost, shared, accessed, altered or destroyed.

Phishing

Phishing is a type of cyber attack where someone attempts to trick users into revealing passwords, financial details or other sensitive information, often through emails, messages or fake websites.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is an additional layer of security which requires a user to provide more than one form of verification before accessing an account.

Filtering

Filtering is technology used to restrict access to inappropriate, harmful or illegal online content.

Monitoring

Monitoring refers to the processes used by schools and the Trust to review activity on devices, networks and online systems for safeguarding, security and operational purposes.

Social Media

Social media refers to websites, apps and online platforms that allow users to create, share and interact with content and with other users.

Digital Citizenship

Digital citizenship refers to using technology responsibly, safely, respectfully and ethically.

Algorithm

An algorithm is a set of instructions or rules followed by a computer system to complete a task or make a decision.

Deepfake

A deepfake is an image, video or audio recording that has been created or altered using AI to make it appear that a person has said or done something that did not actually occur.

Hallucination (AI)

An AI hallucination occurs when an AI system generates information that appears convincing but is inaccurate, misleading or entirely fabricated.

Explainability

Explainability refers to a person's ability to understand how and why an AI system has produced a particular output, recommendation or decision.

Human Oversight

Human oversight means that an appropriately trained person remains responsible for reviewing, checking and making decisions about AI-generated outputs rather than relying solely on the technology.

Safeguarding

Safeguarding refers to the actions taken to protect children, young people and vulnerable adults from harm and to promote their welfare, including protecting them from online risks.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) is the person within a school responsible for leading safeguarding and child protection arrangements.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is the individual responsible for advising the Trust on data protection compliance, monitoring practice and supporting the rights of individuals regarding their personal data.

Appendix B: Photograph and video consent wording and descriptions

The information below is to help parents make active choices about the photograph and video consent they give for their child, and to help older students to understand how their images may be used if consent has been given.

Please note - Some photographs are required for specific school purposes, such as the identification photograph held on Arbor. These uses and their legal bases are explained in our privacy information. The consent choices below cover optional uses and explain what agreeing to or declining each option means.

Consent	Description	Examples of possible uses (please note this is not an exhaustive list)	Phase (Primary, Secondary, All)
XCET Photo and Film - Taking photos/videos	I give permission for the school to take photographs and video recordings of my child during school activities for educational, pastoral and safeguarding purposes.	Photographing a science experiment to evidence practical learning. Recording a class performance so teachers can review students' participation and progress. Taking photographs during a school trip to support student welfare and supervision. Creating evidence for SEND, pastoral or wellbeing reviews where appropriate. Capturing images or footage as part of safeguarding, health and safety, or incident investigations.	All
XCET Photo and Film - Internal School/Trust Use	I give permission for photographs and videos of my child to be used within the School and Trust community, both printed and digital (for example: lesson materials, displays, newsletters, sharing student photos from school events with families, through a secure access folder, internal presentations and Trust communications).	Displaying photographs on classroom or corridor displays. Including photographs in school newsletters distributed to current families. Sharing photographs from Sports Day, school trips or performances with families through a secure parent platform or password-protected folder. Using images in staff training presentations delivered within the Trust. Including photographs in Trust-wide internal communications celebrating student achievements.	All
XCET Photo and Film - External Publicity & Media	I give permission for photographs and videos of my child to be used in external publicity and shared with external media (for example: school or Trust websites, prospectuses, virtual tours, diocesan or education-related publications, and local newspapers). I understand that	Featuring in a school prospectus for prospective families. Appearing on the school's public website. Inclusion in a virtual school tour for admissions purposes. Publication in diocesan magazines, education sector publications or School/Trust recruitment materials.	All

	photographs used in publicity materials may continue to be used beyond this academic year and beyond my child's time at the school until those materials are updated or replaced.	Photographs provided to a local newspaper to celebrate an award, competition win or community project.	
XCET Photo and Film - Social Media	I give permission for photographs and videos of my child to be used on official school or Trust social media channels (for example: X/Twitter, Facebook, Instagram, YouTube) . I understand that content published online or via social media may remain accessible beyond this academic year and beyond my child's time at the school until it is updated or removed.	Photographs from a school production shared on the school's Facebook page. A video of a choir performance posted on the school's YouTube channel. Images from a charity fundraising event shared on Instagram. A post celebrating sporting success on Instagram Short video clips from curriculum enrichment activities published on official school social media accounts.	Secondary Only

How to Record and Manage Consent Choices

Photograph and video consent preferences are recorded and managed through **Arbor**. Once consent has been given or declined on Arbor parents will need to contact the school via email if they wish to change the status of the consent.

When completing the consent form, parents/carers can choose whether to give or withhold consent for each category separately. Consent is not all-or-nothing; each option can be selected independently. Declining one consent category does not automatically prevent the school from undertaking activities covered by another consent category that has been agreed. For example, a parent may permit Internal School/Trust Use but decline External Publicity & Media and Social Media. In that case, photographs may be used internally within the School or Trust but will not be used in external publicity materials or on social media.

Your latest instruction will replace any earlier permission recorded in Arbor. We will confirm when the record has been updated and relevant staff informed.

Where consent is withdrawn:

- If consent is withdrawn for a particular use, we will update our records and stop using new photographs or videos for that purpose as soon as reasonably practicable.
- Existing images published on school-controlled platforms, including school websites and communication channels, will normally be removed as part of the school's ongoing review and update cycle. If you would like a specific historic image removed more promptly, please contact the school directly and we will action the request on a case-by-case basis.
- Materials that have already been printed, distributed or published externally may remain in circulation until they are updated, replaced or withdrawn in accordance with school procedures.

- We cannot necessarily retrieve printed copies that have already been distributed or content that has been copied, shared or republished by third parties.
- Content published through external media outlets, social media platforms or other channels outside the school's direct control may remain accessible after consent has been withdrawn.

Consent for photographs and videos is separate from a student's access to educational technology, learning platforms and other school systems required for the delivery of education, safeguarding and the school's statutory functions.

Please note for safeguarding purposes we require one photograph of every child to be stored securely on Arbor for identification purposes.

Group Photographs and Videos

The school will take reasonable steps to respect the consent preferences recorded by parents/carers when creating and using photographs or videos.

Where a learner does not have consent for a particular use:

- The school will, wherever reasonably practicable, avoid featuring that learner in photographs or videos intended for that purpose.
- Staff may position learners, crop images, select alternative photographs, or use images where the learner is not identifiable.
- In some circumstances, particularly during large events, performances, sporting fixtures, assemblies or whole-school activities, it may not be possible to guarantee that a learner will not appear incidentally within a wider group photograph or video. The school will nevertheless take reasonable steps to ensure that images are only used in accordance with the recorded consent preferences.

Examples:

Consent Status	What This Means
A student has consent for Internal Use only	The student may appear in classroom displays or secure parent communications but will not be intentionally included in photographs selected for external publicity or social media.
A student does not have consent for Social Media	The school will select alternative images, crop photographs where possible, obscure identity where appropriate or avoid publishing images showing that student on social media channels.
A student does not have consent for any publicity use	The school will take reasonable steps not to use the student's image in websites, prospectuses, social media, promotional materials or media releases.
School production or sports day group photograph	The school may take the photograph for educational, pastoral or record-keeping purposes but will only use it in accordance with the consent permissions recorded for the students featured.

Important: Consent preferences apply to the publication and use of photographs and videos. They do not necessarily prevent photographs or videos being taken where this is required for educational, pastoral, safeguarding, security or operational purposes.