



Digital Learning and Digital Citizenship Policy

1	OVERVIEW	2
2	GUIDING PRINCIPLES	2
3	OBJECTIVES OF THIS POLICY	3
4	DEFINITIONS.....	3
5	TEACHING AND LEARNING.....	4
6	RESOURCES	6
7	SCHOOL-MANAGED STUDENT DEVICES (SENIOR SCHOOL)	6
8	INTERNET FILTERING POLICY	7
9	POLICY REVIEW AND APPROVAL	8
APPENDIX 1 TECHNOLOGY USE GUIDELINES		9
APPENDIX 2 GUIDANCE FOR TEACHERS, STUDENTS AND PARENTS FOR THE USE OF VIDEO CONFERENCE CALLS		10
APPENDIX 3 WEB FILTERING GUIDELINES		14

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

1 Overview

- 1.1 At Tanglin, we leverage innovative digital tools that enhance student outcomes. We are committed to preparing our students to actively participate, and to flourish, in a society permeated with technology. This policy highlights and reinforces the need to educate students about the benefits and risks of using technology, and sets out safeguards that are in place to manage their experience.
- 1.2 With access to technology, electronic tools and resources, comes a responsibility to use all devices and access information appropriately. By encouraging everyone to take responsibility for themselves and others in their use of technology, we are fostering a culture of successful digital citizenship in our students, staff and the wider community.
- 1.3 This policy focuses on the use of technology in teaching and learning. The policy is supported by clear, age-appropriate 'Technology Use Guidance', which is shared and regularly reinforced with students in each school as part of the Student Behaviour Policy (see [Appendix 1](#)).
- 1.4 This policy should be read in conjunction with our [AI Principles](#) and other [school policies](#) including the Student Behaviour Policy, Anti-Bullying Policy, Academic Integrity Policy and the Safeguarding and Child Protection Policy.

2 Guiding Principles

- 2.1 We expect Tanglin faculty staff to be confident role models for technology use; they are encouraged to be innovative in using technology to support teaching and learning.
- 2.2 Students are given the opportunity to experience the potential of technology, along with the challenges, in a safe, secure and nurturing environment.
- 2.3 Elements of digital citizenship can be taught explicitly through the curriculum. Other aspects will be learned through the experience of using technology in increasingly diverse contexts.
- 2.4 Students demonstrate an awareness of their learning process and how digital tools support them. Appropriate scaffolding, guidance and support is essential as students progress through the School.
- 2.5 Where Generative AI is used, students learn to apply a critical lens to outputs. AI is used to support students' thinking, not to replace it.
- 2.6 Students are taught behaviours for dealing with inappropriate content online and given a clear support structure for seeking help if they are distressed by online content at home or at school.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

3 Objectives of This Policy

- 3.1 To underscore the importance of the purposeful, respectful, responsible and safe use of technology.
- 3.2 To outline our approach to educating students in the purposeful, respectful, responsible and safe use of technology.
- 3.3 To set out how student access to technology is managed as they progress through the School. This includes guidance and expectations for the use of school-managed student devices in the Senior School (Section 7).

4 Definitions

4.1 Technology.

- 4.1.1 In this policy ‘technology’ refers to information and communications technology hardware and software.

4.2 Digital Tools.

- 4.2.1 In this policy, ‘Digital Tools’ refers to applications (software and online services) that support teaching and learning, including tools used to create, access, organise, communicate and assess learning.

4.3 Artificial Intelligence (AI).

- 4.3.1 In this policy, ‘Artificial Intelligence (AI)’ refers to computer-based systems or features that can generate, analyse, summarise or make recommendations based on data or user input. Some Digital Tools may incorporate AI features.

4.4 Digital Citizenship.

- 4.4.1 Digital Citizenship at Tanglin includes:
 - confident, capable and responsible use of technology at all times.
 - using technology to participate in a variety of activities.
 - using and developing critical thinking skills when online.
 - literacy in the language, symbols and texts of digital technologies.
 - recognising and solving common issues when using technology, including knowing when and how to report inappropriate content or misuse.
 - using technology to relate to others in positive, meaningful and ethical ways.
 - honesty and integrity in the use of technology.
 - respect for privacy and freedom of speech.
 - understanding the rights of digital content creators and consumers.
 - actively promoting the values of digital citizenship and being positive role models for others.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

5 Teaching and Learning

5.1 Digital Citizenship Education

- 5.1.1 The principles of Digital Citizenship and the importance of safe and responsible internet use are modelled and taught by all teachers wherever opportunities arise. They are also taught explicitly, through both the Lifeskills and the Technology/Computing curriculum.
- 5.1.2 Potential issues and strategies for dealing with them are introduced at an age-appropriate level, and in line with the increasing access to technology as students progress through the School.
- 5.1.3 The Technology Use Guidelines ([Appendix 1](#)), including Internet safety advice, form part of the Student Behaviour Policy and are reinforced through all curriculum use of technology.

5.2 How the use of Digital Tools is managed

- 5.2.1 Digital Tools are selected and used to enhance learning. They should be age-appropriate and used where they add clear educational value—for example by improving access, supporting creativity, enabling collaboration, strengthening feedback and assessment, or helping students to practise and demonstrate learning in different ways.
- 5.2.2 Faculty staff will guide students in the use of Digital Tools to support the planned learning outcomes, with due regard for students' age and maturity.
- 5.2.3 Students will be educated in Digital Literacy, including effective online research (knowledge location, retrieval and evaluation). Students will be taught to acknowledge sources and to respect copyright when using digital materials in their own work.
- 5.2.4 Students will be introduced to age-appropriate Generative AI tools, applying Tanglin's AI Principles for purposeful, respectful and safe use of Gen AI, aligned with the Academic Integrity Policy.
- 5.2.5 Emerging technologies and new Digital Tools (including tools that incorporate AI) will be examined for educational benefit before being widely adopted.
- 5.2.6 Any new software must be assessed under the current New Software Procurement Guidelines, to ensure that it meets our standards for data protection and cyber security. A list of approved third-party software is maintained by the Technology Working Group and monitored by the Risk and Compliance Director.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

5.3 How Internet access is managed within the School

- 5.3.1 Faculty staff will guide students in online activities that will support the planned learning outcomes, with due regard for the students' age and maturity.
- 5.3.2 Students will be educated in the skills of Digital Literacy i.e. the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Students will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.
- 5.3.3 Students will be introduced to age-appropriate Generative AI tools, applying Tanglin's [AI Principles](#) for purposeful, respectful and safe use of Gen AI, aligned with the Academic Integrity policy.
- 5.3.4 Infant and Junior students' internet access will be closely supervised.
- 5.3.5 Senior students will be provided internet access according to requirements and with appropriate filtering and monitoring in place (see Section 8)
- 5.3.6 All internet use should be in accordance with the relevant schools' Technology Use Guidelines (see [Appendix 1](#)).
- 5.3.7 Students will be given a clear procedure for reporting unsuitable internet content, along with a clear structure for accessing support if they are distressed by online content, at school or at home.
- 5.3.8 Students are informed that internet use in school is monitored and logged and that these logs can be retrieved under the direction of a Head of Year or member of school Leadership Teams.

5.4 Remote Learning – Audio and Video Conferencing

- 5.4.1 If it is not possible for students to access the school campus, the School may activate 'Remote Learning' for students. At these times, teachers will use the online learning platforms that students are familiar with. This will ensure that students continue to be supported by their teachers, whilst undertaking meaningful learning tasks.
- 5.4.2 Conference calls may also be used when Remote Learning is activated, to enable real time voice or video communication between teachers and students. The School acknowledges that this can create situations where professional and personal boundaries are disrupted. This policy, and the further guidance for staff, parents and students in [Appendix 2](#) aim to ensure that the various technologies available can be used in ways that are effective and safe for everyone.
- 5.4.3 Teachers may terminate a student's participation in a video call if they have any concerns about that student's dress, location, behaviour or supervision.

5.5 How e-safety issues are handled

- 5.5.1 Any breach of the Technology Use Guidance, or the Student Code of Conduct will be dealt in accordance with the [Student Behaviour Policy](#).
- 5.5.2 Cyber-bullying incidents are taken extremely seriously and are dealt with in the same way as any other incidence of bullying (see the [Anti-Bullying Policy](#)).
- 5.5.3 Any concern that an e-safety incident may be an indicator of a child protection issue must be reported to the relevant Designated Safeguarding Lead in line with the [Safeguarding and Child Protection Policy](#).

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

5.6 How electronic communication is managed

- 5.6.1 Each student in the Junior and Senior Schools has a school-based email account, which is specific to their system login.
- 5.6.2 Senior School students are able to send emails internally and externally for school use. Junior School students may use school email for a specific purpose, under supervision and with appropriate guidance.
- 5.6.3 Student emails can be accessed and reviewed at the request of a subject or class teacher, or a parent of the student, with permission from a member of the Leadership Team of the relevant school.

6 Resources

- 6.1 Digital devices, infrastructure, applications and the internet provide opportunities for children to learn in new and interesting ways, often in ways not possible using other resources or approaches.
- 6.2 Tanglin provides a variety of technologies for students and staff to use for learning, both inside and outside the classroom, and on and off campus.
- 6.3 Students are expected to take reasonable care of any technology devices or hardware loaned to them by the School.
- 6.4 Students must discontinue the use of any Tanglin technology platforms and services on leaving the School.

7 School-Managed Student Devices (Senior School)

- 7.1 For students in the Senior School (Years 7–13), the School requires the use of a school-managed device. While parents purchase the device through an approved vendor, the device is configured and managed by the School to ensure a safe, secure and effective learning environment.
- 7.2 School management of student devices supports safeguarding, wellbeing, online safety, academic integrity, and effective teaching and learning.

7.3 Device Management and Security.

- 7.3.1 School-managed devices are configured to:
 - Ensure required educational applications are installed and kept up to date
 - Enforce security settings appropriate for a school environment
 - Apply age-appropriate content filtering
 - Protect student data and reduce the risk of malware or unauthorised access
- 7.3.2 If a device is reported lost or stolen, the School may remotely lock or reset the device to protect information and security.

7.4 Monitoring and oversight.

- 7.4.1 In order to meet its safeguarding and duty of care responsibilities the School may monitor activity on school-managed devices. This may include:
 - Websites visited and the category of those websites
 - The time and duration of access
 - Keyword searches made through enabled search engines
 - Alerts relating to potentially unsafe, harmful or inappropriate content

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

7.4.2 Monitoring is proportionate, purposeful and focused on student safety and wellbeing, rather than routine surveillance of individual behaviour.

7.5 What the School does not monitor.

7.5.1 The School does not:

- Monitor the content of private communications unless a safeguarding concern is identified
- Access personal passwords
- Use monitoring data for commercial purposes

7.5.2 Information accessed through monitoring is handled in line with the School's Confidentiality Policy and Safeguarding and Child Protection Policy.

7.6 Use of monitoring information.

7.6.1 Information from device monitoring may be reviewed by appropriate members of staff (such as safeguarding leads or senior leaders):

- When an alert is generated
- When a concern is raised about student safety, wellbeing or conduct
- As part of an investigation into serious misconduct or safeguarding risk

7.6.2 Where necessary, this information may contribute to pastoral support, safeguarding processes, or disciplinary procedures, always with student welfare as the primary consideration.

7.7 Expectations of students.

7.7.1 Students using school-managed devices are expected to:

- Use their device in a responsible, respectful and lawful manner
- Comply with all School policies relating to behaviour, academic integrity and online conduct
- Respect the purpose of security settings and content filters
- Understand that use of a school-managed device carries a responsibility to act appropriately at all times

7.7.2 Digital citizenship expectations apply during and beyond the school day where device use impacts the wellbeing or safety of others or the reputation of the School.

7.8 Partnership with parents.

7.8.1 The School recognises the importance of working in partnership with parents to support safe and responsible technology use.

7.8.2 Parents are encouraged to:

- Discuss responsible device use with their child
- Support the School's expectations around digital citizenship
- Raise questions or concerns through appropriate school channels

8 Internet Filtering Policy

8.1 The School uses web-filtering technologies to reduce access to particular types of internet content, in accordance with our duty of care to protect our students.

8.2 The Technology Team follow guidance from the whole school Leadership Team in configuring the filtering systems. This is set out in [Appendix 3](#).

8.3 Temporary exemptions can be made where this is related to appropriate schoolwork or research. The procedure for requesting an exemption is set out in [Appendix 3](#).

8.4 Web-filtering does not guarantee internet safety and is complemented by on-going education in digital citizenship and by the vigilance of staff and students.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

- 8.5 The Technology Team will actively monitor network use by students and share reports with the school Leadership Teams highlighting any suspicious activity (including being in school and not logging into the network).

9 Policy Review and Approval

- 9.1 This policy will be reviewed by the Technology Working Group and the whole school Academic Committee at least every two years.
- 9.2 Any significant changes to the policy must be approved by the Education Committee of the Board of Governors.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

Appendix 1 Technology Use Guidelines

Student Responsible Use Guidelines:

[Student Responsible Use Guidelines form part of the Student Behaviour Policy \(Please refer to Appendix 3 at this link\)](#)

For Senior School students, these Responsible Use Guidelines apply equally to personally purchased but school-managed devices, as outlined in Section 7, above.

A note on 'screen time' for children in the Infant School:

Tanglin adheres to the principle that technology should enhance or transform learning and as such we promote a balanced and purposeful use of devices, where quality of interaction is the key consideration via content, context and connections.

Children are taught about self-regulation and responsible use from Nursery onwards, using timers and guided access to help our younger learners manage their screen time and to support focused App use. Screen time is carefully considered in the Early Years, as the learning environment is designed to foster hands-on learning with a wide variety of physical resources and multi-sensory experiences.

As the children mature and devices become more diverse in Year 1 and Year 2, guided access is gradually removed so that children learn to self-moderate. Children are always supervised whilst using devices in the Infant School, and particularly whilst using the internet. Independent screen time may range from a 5 minute visual timer in Nursery up to a single task of 20 minutes in Year 2.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

Appendix 2 Guidance for Teachers, Students and Parents for the use of Video Conference Calls

General

The School acknowledges that the use of video conferencing tools creates a situation where professional School-Family relationships intersect with personal environments. The following guidance is intended to ensure that the experience is effective and safe for everyone.

Parents are encouraged to assist their children in building healthy personal boundaries by ensuring that their children are appropriately dressed for any learning involving video conferencing, and that they are able to participate from a suitable location.

Students are not expected to be in school uniform. Clothing should be in line with what would be deemed appropriate for a school non-uniform day. Pyjamas, swimming costumes or other overly revealing clothing are not acceptable.

The School recognises that students, particularly in the Senior School, are likely to have desks in their bedrooms where they study and this may seem a logical place from which to video conference with their teachers. Bedrooms are however, considered highly personal environments. In accordance with the School's commitment to educating students about appropriate personal boundaries, the School discourages students from using their bedrooms as locations for remote learning video conferencing.

The School recommends that students participating in video conferencing:

- Use family spaces rather than private spaces.
- Consider using digital tools that blur or obstruct backgrounds to protect their family's privacy where these are available.

Staff, parents and students should all take care that any setting visible to others on the call

- Does not contain material that any reasonable person would find offensive in relation to race, religion, culture or gender, or any otherwise inappropriate material.
- Does not contain any highly personal items or information that may allow unreasonable line of sight into personal life.

School Specific Guidance:

Infant School

Teachers:

- You must not accept any meeting requests from parents or children. All class meetings should be initiated as scheduled meetings in the children's MS Teams calendar.
- In terms of safeguarding, if you see anything concerning during the meeting, please follow safeguarding procedures as you would in school.
- You must not record or capture images from any video conferencing sessions.
- Any video conferencing should be scheduled rather than ad hoc video call connections.
- Please ensure you are dressed professionally, even if working from home.
- Please ensure that your background does not compromise your privacy or location – consider using the blur background feature or a virtual background available in Teams.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

- Please ensure you are never one-to-one on Teams with a child – in a group conference, a supervising adult in the home should be visible for each child at the start of the call.
- Please begin each conference with a reminder about expectations during the meeting. Pre-set your meeting to mute children’s microphones to start while you introduce and set out the expectations in line with our technology use guidelines. Use hands up initially for children to indicate that they would like to share something.

Parents:

- Please ensure your child and any others in the household who may be visible during the conference are appropriately clothed.
- The device used must be set up in a communal room and an adult must be visible at the start of the call – teachers reserve the right to remove any child who they believe to be alone.
- Please ensure that the background visible behind your child does not compromise your privacy or location – as an alternative a virtual background is available within the Teams software.
- Please note that these conferences are specifically for children and their teacher to catch up – if you need to speak to the teacher, please arrange an appropriate time via email and please respect the privacy of other children who may contribute during the call.
- Please note that recording or image capturing of the conferences is not allowed.

Children

- You must always have a grown up in the room when you are using an internet connected device.
- Make sure you are fully dressed.
- Remember, we should communicate online in exactly the same way as if we were talking face to face. THINK before you speak.
- Follow the same rules as when you are in school. Hands up and don’t shout out. (Remember you will be on mute to begin with and the teacher will allow you a turn to speak)
- We expect the same outstanding standards of behaviour as when you are in class.
- You must not record or take photos of the video session.

Junior School

Teachers

- You must not accept any meeting requests from parents or children. All class meetings should be initiated as scheduled meetings in the children’s MS Teams calendar.
- In terms of safeguarding, if you see anything concerning during the meeting, please follow safeguarding procedures as you would in school.
- You must not record or capture images from any video conferencing sessions
- Any video conferencing should be scheduled rather than ad hoc video call connections.
- Please ensure you are dressed professionally, even if working from home.
- Please ensure that your background does not compromise your privacy or location – consider using the blur background feature or a virtual background available in Teams.
- Please ensure you are never one-to-one on Teams with a child – in a group conference, a supervising adult in the home should be visible for each child at the start of the call.
- Please begin each conference with a reminder about expectations during the meeting. Pre-set your meeting to mute children’s microphones to start while you introduce and set out the expectations in line with our technology use guidelines. Use the hands up feature initially for children to indicate that they would like to share something.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

Parents

- Please ensure your child and any others in the household who may be visible during the conference are appropriately clothed.
- The device used must be set up in a communal room and an adult must be visible at the start of the call – teachers reserve the right to remove any child who they believe to be alone.
- Please ensure that the background visible behind your child does not compromise your privacy or location as all participants in the conference will be able to see your child and his/her surroundings – as an alternative a virtual background is available within the Teams software.
- Please note that these conferences are specifically for children and their teacher to catch up – if you need to speak to the teacher, please arrange an appropriate time via email and please respect the privacy of other children who may contribute during the call.
- Please note that recording or image capturing of the conferences is not allowed.

Students

When using MS Teams at home:

- Remember, we should communicate online in exactly the same way as if we were talking face to face. THINK before you speak.
- Make sure you are fully dressed.
- Follow the same Responsible Use Guidelines as you would in school.
- Keep your video switched on at all times during the Teams call.
- You must always have a grown up in the room when you are using video.
- We expect the same outstanding standards of behaviour as when you are in class.
- You must not record or take photos of the video session.

Senior School

Teachers

- You must not accept any video meeting requests from parents or students. All class meetings should be set up by the teacher, through MS Teams.
- In terms of safeguarding, if you see anything concerning during the meeting, please follow safeguarding procedures as you would in school.
- Please ensure you are dressed professionally, even if working from home.
- Please ensure that your background does not compromise your privacy or location – as an alternative your background can be blurred in Teams software.
- Avoid one-to-one video calls with students unless you are conducting an assessment that can only take place one to one such as a Languages oral or an IA*. If only one student has joined a scheduled class call, please terminate the call and reschedule.
- Please remind students that normal school expectations of behaviour apply during a remote learning session.

*Where one to one sessions are required, parents must have given separate, specific permission and an audio recording must be made, for safeguarding purposes.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

Students

- Ensure that you are in a quiet, distraction-free environment where possible.
- Make sure you are fully dressed in clothing that would be appropriate for a non-uniform day in school.
- Make sure that there is nothing inappropriate on display in your background. If any offensive or inappropriate material can be viewed, you will immediately be rejected from the call.
- We advise that you are in a communal space rather than your bedroom. If your workstation is in your bedroom, make sure you are sitting at a desk (rather than on your bed) and have your bedroom door open.
- Before you join the call, ensure that you don't have email, websites or apps open that aren't related to learning. Turn off other notifications. We also advise you to put any other device such as a phone in another room. All of this will help you to avoid distractions and focus on the call.
- Keep your language, behaviour and actions appropriate for class. This includes your communication during the call, whether spoken or via the chat feature.
- Follow the same Responsible Use Guidelines as you would in school.
- You should always start with your microphone off. This will help to avoid any confusion about who is speaking and ensure there isn't a chaotic start with numerous students speaking at once.
- Using headphones often helps with audio clarity.
- On no account should any recording or photograph of the chat be made by a student, whether through the Teams app or via another device pointed at the screen (such as your phone camera).

These guidelines are designed to keep us all safe in this remote learning environment. If you do not abide by them, you risk having access to further Teams calls suspended.

Parents

Please note that these conferences are specifically for the teacher to address learning issues with the class. If you are in the room with your child, please remain a silent observer of the meeting and respect the privacy of other students.

- All images transmitted during video conferences will be used for the purpose of carrying out the video conference then in session.
- Please note that recording or image capturing of the conferences is not allowed.
- The School will not record any video conference with students unless parents have been informed and given specific consent beforehand.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028

Appendix 3 WEB FILTERING GUIDELINES

The Technology Infrastructure Team follow the following guidance which has been approved by the whole school Leadership Team:

- Where possible enforce Safe Search in web search engines
- Restrict access to websites that fall under the following categories (as defined by the filtering software)

• Abortion • Adult mature / content • Alternative spirituality / belief • Chat / IM / SMS • Child pornography • Controlled substances • Extreme • Gambling • Games • Hacking	• Humour / jokes • Intimate apparel / swimwear • Malicious websites • Marijuana • Nudity • Peer to peer • Personal / dating • Phishing • Piracy / copyright concerns • Pornography • Proxy avoidance	• Scam / questionable / illegal • Sex education • Sexual expression • Social networking • Spam • Suspicious • Violence / hate / racism • Weapons
---	--	---

Filtering Order

Where a site is classified under more than one category by the Internet filters, the more restrictive policy shall apply.

Process for allowing/blocking access to an individual site

If a teacher requires an individual site to be blocked or unblocked for legitimate educational purposes, then they should submit an email to Technology Help Desk requesting access and a very brief overview of the reasoning. This is for record keeping purposes. The site will then be reviewed for security concerns by the Technology Team. Any concerns will be raised with the requesting teacher and/or their respective School Leadership Team.

A log of the requests will be available for the Leadership Teams of each school to review.

Process for review of the categories or policy

The filtering categories are subject to review and different filtering policies may be put in place for particular year groups, where appropriate.

If a staff member wishes to have the categories or policy reviewed, they should first approach the Leadership Team of their individual school.

If the Leadership Team of the school concerned approves the request, it would then be submitted to the Director of Technology to be implemented, subject to any technical issues.

Any change that will affect the whole school must be discussed by the TWG and approved by the whole school Leadership Team.

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	EC - May 2026	April 2026	TWG; Academic Committee	May 2028