St Dunstan's College

Senior School



IT Policy

Policy Owner: Deputy Head (Pastoral)

ISSR Reference: N/A

Reviewed: Michaelmas 2025

Approved: Full Governing Body Michaelmas 2025

Next Review: Michaelmas 2026

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Creation of new policy	Chief Operating Officer	Michaelmas 2024	New policy
Interim review	Chief Operating Officer	Trinity 2025	Review of roles and responsibilities
Annual review	Chief Operating Officer	Michaelmas 2025	None

Contents

1. Aims and introduction 4
2. Legislation 4
3. Roles and responsibilities 5
4. Educating students about online safety 7
5. Educating parent / carers about online safety 9
6. Cyber-bullying 9
7. Acceptable use of the internet in school and outside of school whilst using school devices 11
8. Pupils using mobile devices in school 12
9. How the school will respond to issues of misuse by students 13
10. Training 13
11. Monitoring arrangements 14
12. Links with other policies 14
Appendix A: Student Acceptable Use Agreement 15
Appendix B: Bring your own device 17

1. Aims and introduction

1.1 Policy aims

This policy is applicable to students and parents / carers of St Dunstan's College Senior School (the school).

The school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers the school to protect and educate the whole school community in its use of technology, including mobile and smart technology, which in this policy is referred to as 'mobile phones'
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate.

1.2 Approach to online safety: risk categories

The school's approach to online safety is based on addressing the following categories of risk:

Content	Being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
Contact	Being subjected to harmful online interaction with other users, such as peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct	Personal online behaviour that increases the likelihood of, or causes, harm such as making, sending and receiving explicit images, e.g. consensual and non-consensual sharing of nudes and semi-nudes, and / or pornography, sharing other explicit images and online bullying.
Commerce	Risks such as online gambling, inappropriate advertising, phishing and / or financial scams.

2. Legislation

This policy is based on advice from the Department for Education (DfE's) statutory safeguarding guidance, Keeping Children Safe In Education and informed by the following legislation:

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: advice for teachers and school staff

- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DFE's guidance on protection of children from radicalisation and reflects legislation, including but not limited to the Education Act 1996 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is 'a good reason' to do so.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

The governing body has ultimate responsibility for monitoring this policy but will delegate day-to-day responsibility to the Chief Executive Officer (CEO) and the Head of St Dunstan's Senior School.

The governing body has a duty to ensure that:

- All staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- Attend annual meetings with the Designated Safeguarding Lead (DSL) to discuss online safety, requirements for training and to review online safety logs provided by the Director of Digital Services
- All students are taught how to keep themselves and others safe, including keeping themselves safe online
- That the school has appropriate filtering and monitoring systems in place on school devices and school networks, and to annually review their effectiveness. This includes assessing the following requirements:
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing and monitoring provision at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs.

The governor who oversees online safety is the Safeguarding Link Governor.

3.2 The Head of St Dunstan's Senior School

The Head of St Dunstan's Senior School is responsible for ensuring that staff in St Dunstan's Senior School understand this policy, and that it is being implemented consistently across the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in the Child Protection and Safeguarding Policy. The DSL takes the lead responsibility for online safety in the Senior School, including:

- Supporting the Head of the Senior School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of the Senior School and governing body to review this policy annually and to ensure that the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring and systems and processes that are in place
- Working with the Director of Digital Services to ensure that appropriate systems and processes are in place
- Working with the Head of St Dunstan's Senior School, Director of Digital Services and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding and Child Protection Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Expected Pupil Behaviour Policy
- Updating and delivering staff training on online safety at least annually
- Liaising with other agencies and / or external services if necessary.

3.4 The Director of Digital Services

The Director of Digital Services is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Testing the school's filtering and monitoring systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that online safety incidents are logged and dealt with appropriately in accordance with this policy.

3.5 Staff

All staff, including contractors and agency staff, and volunteers, as appropriate, are responsible for:

- Maintaining an understanding of this policy
- Agreeing to the staff terms on acceptable use of the school's IT network and internet (Electronic Information and Communication Systems Policy) and ensuring that students follow the school's student terms on acceptable use (Appendix A)
- Knowing that the DSL is responsible for the filtering and monitoring of systems and processes, and being aware of how to report incidents or processes failing by raising an alert on CPOMs, or alerting the Digital Services team
- Following the correct procedures, by contacting the Digital Services team, if they need to bypass the filtering and monitoring system for education or work purposes
- Working with the DSL to ensure that online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are deal with appropriately in line with the school's Expected Pupil Behaviour Policy
- Responding appropriately to reports and concerns about sexual violence and / or harassment, both online and offline, and maintaining an attitude of 'it could happen here.'

3.6 Students, parents and carers

Students, parents and carers are expected to:

- Read, understand and agree to the terms on acceptable use of the school's IT systems and networks (Appendix A).
- Engage with any e-safety training and advice provided.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum, the learning outcomes at each stage will be:

Lower School	Understanding a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy. Recognising inappropriate content, contact and conduct and how to report concerns. How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours. About the harms and benefits of social media. The sharing and viewing of indecent images of children (including those created by children) is a criminal offence that carries severe penalties including prison. Not to provide material to others that they would not want shared further and not to share personal material that is sent to them. Rights, responsibilities and opportunities online, including that the same expectation of behaviour apply in online contexts. Online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online. How information and data is generated, collected, shared and used online. That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours and can be harmful. How to assess whether information and news online is reliable. How to spot if an adult poses a threat to you, and about grooming, exploitation and coercion. That AI has pros and cons and the age restrictions in place for using it.
Middle School	To understand how changes in technology affect safety, includes new ways to protect online privacy and identity. How to report a range of concerns. The impact of viewing harmful content. That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people seem themselves in relation to others, and negatively affect how they behave towards sexual partners. What to do and where to get support to report material or manage issues online. Understanding Extremism and Radicalisation and how these can take place online. That AI has pros and cons, and the age restrictions in place for using it, alongside learning about AI and Academic Integrity.
Sixth Form	That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people seem themselves in relation to others, and negatively affect how they behave towards sexual partners. What to do and where to get support to report material or manage issues online.

	The sharing and viewing of indecent images of children (including those created by children) is a criminal offence that carries severe penalties including prison. That AI has pros and cons, and the age restrictions in place for using it, alongside learning about AI and Academic Integrity.

5. Educating parent / carers about online safety

The school will raise parents / carers' awareness of internet safety in letters, or other communications home, and also offer at least one annual parent e-safety session. This information will include:

- What systems the school uses to filter and monitor online use
- What students are asked to do online, including the sites they will be asked to access.

Concerns or queries about this policy should be raised with the relevant form tutor in the first instance. Further advice may be sought from the DSL.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, the school will ensure that students understand what it is and what to do if they become aware of it happening to them or others. Students will be taught how they can report any incidents and will be encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with students explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

As part of wider safeguarding training, all staff, governors and relevant volunteers receive training on cyber-bullying, its impact and ways to support students (see Section 10).

The school also sends information/ on cyber-bullying to parents/carers so they are aware of the

signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Expected Pupil Behaviour Policy.

Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. The DSL will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

As detailed in the school's Expected Pupil Behaviour Policy, the CEO, the Head of the Senior School, and any member of staff authorised to do so by these two role holders, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and / or;
- Is identified in the school Expected Behaviour Policy as a banned item for which a search can be carried out, and / or;
- Is evidence in relation to an offence.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member must reasonably suspect that the device has, or could be used to:

- Cause harm, and / or;
- Undermine the safe environment of the school or disrupt teaching, and / or;
- Commit an offence.

If inappropriate material is found on the device, the DSL will decide on a suitable response in accordance with the school's Expected Pupil Behaviour Policy. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that is continued existence is likely to cause harm to any person, and / or

- The student, or the parent / carer refuses the delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they must:

- **NOT** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide on what to do next, in accordance with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's Expected Pupil Behaviour Policy.

Any complaints about searching for, or deleting, inappropriate images or files on student's electronic devices will be dealt with through the St Dunstan's Education Group's Complaints Policy and Procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The school recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography, i.e. pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully students in line with the Expected Pupil Behaviour and Anti-Bullying policies.

Staff are made aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school and outside of school whilst using school devices

All students, staff, volunteers and governors are expected to sign an agreement regarding the

acceptable use of the school's IT systems and the internet. Visitors are expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The school will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. The following systems are in place to enable the school to monitor and filter web content and emails.

Web filter	New Sweeper
Monitoring software for student devices, on and off site	Senso
Anti-virus software	Bit Defender GravityZone
Third-party spam filter	Microsoft 365 Advanced Threat Protection

These systems are provided by third-party companies who also ensure the usability, uptime and availability of these systems. Any person that logs onto a device and joins a school network will pick up the filtering and monitoring system for the school the device is being used at.

8. Pupils using mobile devices in school

By bringing an internet capable device to school, all students agree to the following rules:

- In Years 7-11, students must keep phones and smart watches locked in a Yondr pouch when in school, or on a school-based activity.
- In the Sixth Form, students are permitted to use their mobile phones, in line with the rules below, in the Sixth Form Cafe and study area only.
- Use of personal devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher. Laptops are available for students to use in classrooms for learning activities that require digital devices, which can be booked out via Digital Services by teachers. This should be the primary form of providing digital devices to students in the classroom outside of the Sixth Form.
- When they are used, the primary purpose of the use of personal devices at the school is educational.
- If a student is given permission to use a personal device during a normally 'banned' time they may only use the device for the purpose stated by the staff member granting the permission. Students must make no attempts to circumvent the school's network security and / or filtering policies. This includes setting up proxies and downloading programmes to bypass security.

- Students must not make or distribute pictures or video of students or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting an image or video online).
- Students must only access the internet via the school wireless network whilst onsite. Students must not access the internet using their mobile networks, as these are unfiltered and thus contravene the Acceptable Use Agreement.

Further detail on Bring Your Own Device is included in Appendix B.

9. How the school will respond to issues of misuse by students

Where a student misuses the IT systems or internet, the school will follow the procedures set out in the Expected Pupil Behaviour and IT Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training annually as part of safeguarding training, as well as relevant updates as required, for example through emails, briefings and CPD sessions. Staff are expected to understand that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Physical abuse, sexual violence and initiation / hazing type violence can contain an online element
- Children can abuse their peers online through:
- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and / or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise the dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and their deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in the school's Child Protection and Safeguarding Policy.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety and these are reviewed by the governing body termly. This policy will be reviewed by the Designated Safeguarding Lead, Director of Digital Services and the COO annually. At every review, the policy will be approved by the Education Committee.

12. Links with other policies

This IT Policy links to the following policies:

- Expected Pupil Behaviour [school]
- Information Security [Group]
- Safeguarding and Child Protection [school]

Appendix A: Student Acceptable Use Agreement

Pupil Acceptable Use Agreement

I understand that I must use St Dunstan's College's (the school) systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

I agree to follow the rules below when using IT at school (SDC) and at home (H):

- I will only use IT at school for educational purposes. (SDC)
- I will not access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- I will only use my login and password and never share these with others. (SDC) (H)
- I will always log off, or shut down, a device when I've finished working on it. (SDC) (H).
- I will not connect a memory stick or other storage device (including phones and tablets) to a school computer. (SDC)
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher. (SDC)
- I will only open files intended for me and delete my own files. (SDC)
- The messages I send (including emails, instant messages, Snapchat, Instagram, etc.) will be polite and sensible. (SDC) (H)
- I will never give out my own or other people's name, address (including email) or phone number online without the permission of my teacher, or parent / carer. (SDC) (H)
- I will not upload any images of school activities to any social networking site. (SDC) (H)
- I will not deliberately look for, save or send anything that could be construed as obscene, hateful, threatening or offensive. (SDC) (H)
- I understand that sending a message with the deliberate intention of making another person feel offended, embarrassed, threatened, or hurt is bullying, and will be dealt with according to the school's Anti-Bullying Policy. (SDC) (H)
- If I see anything I am unhappy with on the computers or other devices, I will turn the screen off and tell a member of staff, my parent / carer or other appropriate adult straight away. (SDC) (H)
- I understand that the school can check my computer or other devices and that my parents/carers can be contacted if staff are concerned about my online safety.
- I understand that I must check my school email account regularly (at least once per day) and that I must attempt to respond to or acknowledge email messages in a timely manner. (SDC) (H)
- I understand that the sanctions for misuse of IT will be in line with the Expected Pupil Behaviour Policy, and may include a call-back, detention, restriction of IT privileges or more

serious sanctions for actions such as bullying or possessing or sending offensive material. (SDC) (H)

- If I bring a mobile phone or other personal electronic device into school, and I am in Years 7-11, I will keep them locked in a Yondr pouch, when in school or in a school-based activity. (SDC)
- If I bring a mobile phone or other personal electronic device into school, and I am in Year 12 or 13, I will only use the device in the Sixth Form Café or Study Area, and always in accordance with this Acceptable Use Agreement.

Pupil Name: _____ Form: _____

Pupil Signed: _____ Date: _____

Parent / carer Signed: _____ Date: _____

Appendix B: Bring your own device

Bring Your Own Device (BYOD) St Dunstan's Senior School

GENERAL INFORMATION

Access to the St Dunstan's College (the school) wireless network, whether with school-provided or personal devices is filtered and monitored in compliance with Keeping Children Safe in Education (KCSIE).

Any use of the wireless network entails personal responsibility and compliance with all school rules, and particularly the Student Acceptable Use Agreement.

Sixth Form students are expected to have an internet capable device with them for academic lessons. The school does not expect students outside of Sixth Form to have personal internet capable devices to access the curriculum; teachers are encouraged to utilise digital technology in the classroom to further the learning of students and will request student devices from Digital Services for any such lessons. There are also several banks of student devices positioned in departments across the school site.

RULES FOR STUDENTS USING PERSONAL INTERNET CAPABLE DEVICES

By bringing an internet capable device to the school, all students agree to the following rules:

- Use of personal devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher. Laptops are available for students to use in classrooms for learning activities that require digital devices, which can be booked out via IT Services by teachers. This should be the primary form of providing digital devices to students in the classroom outside of the Sixth Form.
- When devices are used, the primary purpose of the use of personal devices at school is educational.
- The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt lessons in any way.
- The use of personal devices falls under the school's IT Policy and Acceptable Use Agreement, which must be understood and signed by the student before being using any the school's IT network and systems. These documents are found in the Student Handbook and on the school VLE, accessible through Microsoft Teams.
- Pupils must not use personal devices:
    - In the school's corridors
    - In the Refectory

    - During assemblies, lessons or tutor periods (without permission from the relevant staff member)
    - Whilst on school trips, including sports fixtures (without permission from the relevant staff member)
    - Whilst participating in Forder Activities (without permission from the relevant staff member)
- If a student is given permission to use a personal device during a normally 'banned' time (see list above), they must only use the device for the purpose stated by the staff member granting the permission.
- Students must make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programmes to bypass security.
- Students must not make or distribute pictures or video of pupils or staff without their permission, distribution can be as small as emailing/texting to one other person or as large as posting an image or video online.
- Pupils must only access the internet via the school's wireless network whilst at school. Students must not access the internet using their mobile networks, as these are unfiltered and thus contravene the school's IT Policy and Acceptable Use Agreement.
- In Years 7-11, students must keep phones and smart watches locked in a Yondr pouch when in school, or on a school-based activity.
- In the Sixth Form, students are permitted to use their mobile phones, in line with the above rules, in the Sixth Form Cafe and study area only.

CONSEQUENCES FOR MISUSE

'Misuse' includes violating any of the above rules or failing to abide staff instruction with respect to the use of their personal device. One or more of the following sanctions may apply:

- Students may receive a verbal warning, call-back, conduct detention or a serious sanction in line with our Exclusions Policy depending on the circumstance of the offence.
- Students may have access to the school's wireless network removed.
- Students may have a device taken away for the duration of a lesson, activity or event as appropriate.
- Students may have a device taken away and kept in the College Office until a parent/carer collects it.
- Students may have the privilege of bringing a personal device to school revoked.

Serious or repeated misuse of internet capable devices is regarded as a serious offence within the School Rules, and will be dealt with in accordance with the school's Policy on Expected Pupil Behaviour and College Rules.

LIABILITY STATEMENT

Students bring their devices to use at school at their own risk. Students are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be

responsible for the upkeep and protection of their device, including keeping it charged, installing updates or upgrades and fixing any software or hardware issues.

The school is in no way responsible for:

- Personal devices that are broken whilst at school or during school-sponsored activities
- Personal devices that are lost or stolen at the school or during school-sponsored activities.