E-Safety and Mobile Devices Policy

Owner	Deputy Headteacher
Reviewers	Deputy Headteacher, SLT
Approved by	Executive Director
Date approved	August 2026
Next Review Due	August 2027

The E-Safety and Mobile Devices Policy relates to other policies including those for Computing, Safeguarding and Child Protection, and Behaviour, including the Anti-Bullying Policy. It has been agreed by the senior leadership team. It will be reviewed annually.

This policy must be read together with the ISO Safeguarding and Child Protection Policy and follows Keeping Children Safe in Education (2026). Online safety is part of safeguarding. Any online concern about a child's safety or welfare must be reported to the DSL or Safeguarding Team members and recorded on the MyConcern platform.

TEACHING AND LEARNING

WHY IS INTERNET AND DIGITAL COMMUNICATION USE IMPORTANT?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

HOW DOES THE INTERNET BENEFIT EDUCATION?

- access to worldwide educational resources including museums and art galleries;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data.

HOW WILL INTERNET USE ENHANCE LEARNING?

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students provided through Securly
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.

- Staff will guide students in online activities that will support the learning outcomes planned for the students' age and maturity.
- Students at Key Stage Three and Four will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

HOW WILL STUDENTS LEARN TO EVALUATE INTERNET CONTENT?

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to a member of the SLT in the first instance , so that the site can be blocked through Securly. If the content raises a concern about a child's safety or welfare, it must also be reported to the DSL.
- The school will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

HOW WILL EMAIL BE MANAGED?

- Students may only use approved email accounts on the school system and the forwarding of chain mail letters is not permitted.
- Students must immediately tell a teacher if they receive an offensive email. The teacher will report any safeguarding concern to the DSL.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts may be blocked.
- E-mail sent to an external organization by a student, will be written carefully and authorized before sending, in the same way as a letter written on school headed paper.

HOW WILL WEB SITE CONTENT BE MANAGED?

- The point of contact on the website will be the school address, school email and telephone number. Staff or students' home information will not be published.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Website.
- The Executive Director or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

SOCIAL NETWORKING

WHAT ARE NEWSGROUPS AND E-MAIL LISTS?

- Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated.
- If this is demonstrated, the school will control access to social networking sites, and consider how to educate students in their safe use.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students will not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students will only invite known friends and deny access to others.

CAN CHAT BE MADE SAFE?

- Students will not be allowed access to public or unregulated chat rooms including those in online games.
- Children will use only regulated educational chat environments.
- A risk assessment will be carried out before students are allowed to use a new technology in school.

HOW CAN EMERGING INTERNET APPLICATIONS BE MANAGED?

- Emerging technologies, including AI tools will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Primary students are not allowed to bring; mobile phones, smart watches, game consoles. For secondary students mobile phones, smart watches may only be brought to school as set out in the Mobile Device Policy below. The sending of abusive or inappropriate text messages is forbidden and where instances occur will be treated as if the incident took place in school.
- Staff will be issued with a school phone where contact with students or parents is required.

HOW WILL THE RISKS BE ASSESSED?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can not accept liability for the material accessed, or any consequences of Internet access.

In line with KCSIE, the school considers online risks in four areas: content (harmful material), contact (harmful contact with others), conduct (harmful online behaviour) and commerce (online scams, gambling).

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under Romanian Law.

Methods to identify, assess and minimize risks will be reviewed regularly.

The Director will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

HOW WILL FILTERING AND MONITORING BE MANAGED?

From the 2026–27 academic year, ISO uses Securly as its filtering and monitoring system, alongside the Google Admin Console and Microsoft Admin Center. Securly filters internet access on the school network and school-managed devices according to the age and needs of students.

Technical responsibility for the configuration, maintenance and checking of filtering and monitoring systems sits with the IT Manager. This includes ensuring that filtering remains operational, responding to technical failures, making approved changes to filtering settings and supporting investigations where users attempt to bypass filtering.

The Designated Safeguarding Lead (DSL) has safeguarding oversight of filtering and monitoring arrangements. The DSL works with SLT and IT support to ensure that filtering and monitoring appropriately reflect the safeguarding needs of the school.

Securly generates alerts where activity may indicate a risk to a student's safety or wellbeing, including concerns relating to self-harm, bullying, extremism or inappropriate content. Safeguarding alerts are received by the DSL. Alerts will be reviewed promptly and, where they indicate a safeguarding concern, action will be taken in accordance with the Safeguarding and Child Protection Policy and the concern and actions taken will be recorded on MyConcern.

Where staff or students discover unsuitable content that has not been blocked, the URL and relevant details must be reported to the person responsible from the IT so that the filtering arrangements can be reviewed. Where the content raises a concern about a student's safety or welfare, it must also be reported immediately to the DSL.

The school will carry out and record regular checks of its filtering and monitoring arrangements. These checks will confirm that filtering is operating correctly, appropriate categories of content are being blocked, monitoring alerts are functioning and different user groups have appropriate levels of access. Additional checks will be undertaken following significant changes to devices, networks, software or filtering settings.

Filtering and monitoring arrangements will be formally reviewed at least annually by the DSL, SLT and IT support/provider, and additionally following any significant safeguarding incident or major change to the school's technology systems. The review will consider current and emerging online risks, the effectiveness and limitations of the systems and whether any changes are required.

The school will retain appropriate records and evidence, including:

- records of filtering and monitoring checks;
- relevant monitoring reports and alerts;
- safeguarding concerns and actions recorded on MyConcern;
- records of significant filtering changes or technical failures; and
- the annual filtering and monitoring review and any resulting actions.

HOW WILL THE POLICY BE INTRODUCED TO STUDENTS?

- Rules for Internet access will be posted in all rooms where computers are used.
- Instruction in responsible and safe use will take place at the start of each year using the National Online Safety Scheme of work, reminders will precede Internet access.
- Students will be reminded of the rules and risks at the beginning of any lesson using the Internet
- A module on responsible Internet use will be included in the Computing lessons and other appropriate subject areas, covering both school and home use.
- E-Safety rules will be reinforced regularly as opportunities present themselves during Assemblies, parent meetings, lessons etc.
- Students will be informed that network and Internet use will be monitored through Securly.
- Students are taught to tell a trusted adult or a member of the safeguarding team if they see anything online that worries them.
- An ongoing programme of training in e-Safety will take place within the school to keep abreast of new risks and threats.

HOW WILL STAFF BE CONSULTED?

- All staff are governed by the terms of the 'Responsible Internet Use' in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School E-Safety Policy, and its importance explained.
- Staff will be made aware that Internet traffic can be monitored through Securly and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by the senior leadership team and DSL.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required, as part of annual safeguarding training
- Staff must report any online safety concern about a student to the DSL and record it on MyConcern.
- Staff will understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must not use personal phones, emails or social media to communicate with parents or students
- Staff must not use personal devices to take photographs or videos of students.

HOW WILL ICT SYSTEM SECURITY BE MAINTAINED?

- Personal data sent over the Internet will be encrypted or otherwise secured however the school cannot be held responsible for the use of secure passworded sites from within school. The school's security measures may not prevent losses due to key logging or data theft when people access online banking/emails etc on the school system.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to email.

HOW WILL COMPLAINTS REGARDING INTERNET USE BE HANDLED?

- Responsibility for handling incidents will be delegated to the senior leadership team.
- Any incident that raises a safeguarding concern, including online abuse, cyberbullying, grooming, radicalisation or the sharing of nude or semi-nude images, will be immediately referred to the DSL and managed under safeguarding policy.
- Any complaint about staff misuse must be referred to the Executive Director and will be managed accordingly.
- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with staff to resolve issues.

- As with drug issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. This decision will be taken by the Executive Director and DSL.

Sanctions available include:

- reporting incident on Toddle following the Behaviour policy steps and on MyConcern where there is a safeguarding concern.
- informing parents or carers;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

HOW WILL PARENTS' SUPPORT BE ENLISTED?

- Parents' attention will be drawn to the School E-Safety Policy in the parents handbook.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organizations such as Child Exploitation and Online Protection (CEOP) and the Romanian national helpline (119)
- The school will maintain a list of e-safety resources for parents/carers.

HOW IS INTERNET USED ACROSS THE COMMUNITY?

- Adult users will need to sign the acceptable use policy.
- Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.
- The school will liaise with local organizations to establish a common approach to e-safety.

MOBILE DEVICE POLICY

Rationale

We are committed to providing a caring, friendly and safe environment for all of our students and believe that modern technology in the form of mobile devices, when used appropriately, can enhance student's learning within School. We are also clear that when mobile devices are used inappropriately, they distract from the core school business of learning, and at worst can be used as a tool for bullying or abuse.

In order to strengthen our Safeguarding and Child Protection practices and to reduce risk for all of our community, ISO implements the following policy with regard to Mobile Devices.

Policy

• Mobile phones, smart watches are not allowed to be brought into school by EY and Primary students. An exception for this will be made for students who have been given permission to leave school alone at the end of the day and KS3-5 students. In this event, the student should leave their devices at the reception of the school in the designated shelf and basic models should be considered by the parents as the school can not be held to account for any loss or damage.

• If a student needs to call home, s/he will gain permission from their class teacher for them to attend the reception/secretary/ nurse to make the call.

• A student found with a mobile device at a time (apart from the immediate arrival or departure to/from school) will have their device withheld. Repeating this action will lead to disciplinary sanction.

• ISO provides electornic devices to students to support their learning. Electronic devices are considered a valuable aid to learning and will be permitted to be used in class only with the express permission of the teacher. Such devices must only connect to the internet via the school's Wi-Fi, which is filtered and monitored through Securly. They must not have a separate facility for access via a commercial mobile data network.

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile device and a serious breach of the school's behaviour policy resulting in sanctions being taken.

• Photographing, filming or recording in lessons without permission.

• Photographing or filming staff or other students without their knowledge or permission.

• Photographing or filming in toilets, changing rooms and similar areas.

Taking, sharing or requesting nude or semi-nude images or videos. These incidents will always be referred to the DSL.

• Bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites.

• Refusing to switch a device off or to hand over the device at the request of a member of staff.

• Using the device outside school hours to intimidate or upset staff and/or students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

Withholding procedure

• When a mobile device is withheld by a member of staff it will be handed to the designated member of the SLT.

If staff believe a device contains content that raises a safeguarding concern, it will be handed directly to the DSL. Staff must not view, copy or forward any images, videos or messages.

• The device will only be returned to the student's parent or legal guardian after the policy breach has been discussed.

• Repeated offences may result in the student being referred to the Executive Director for more serious sanctions which may include the possibility of the permanent withdrawal from the school.

- SLT members have the right to search students' bags, pockets, lockers without any prior notice if there is a reasonable concern for safety, security or breach of school rules. Searches will be carried out by two members of staff and parents will be informed. The contents of a device will not be searched by staff. Any concern about the content will be reffered to the DSL.

KS1

To stay **SAFE online and on my devices**, I follow these rules:

	✔
I only **USE** devices or apps, sites or games if a trusted adult says so	
I **ASK** for help if I'm stuck or not sure	
I **TELL** a trusted adult if I'm upset, worried, scared or confused	
If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
I look out for my **FRIENDS** and tell someone if they need help	
I **KNOW** people online aren't always who they say they are	
Anything I do online can be shared and might stay online **FOREVER**	
I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
I don't change **CLOTHES** or get undressed in front of a camera	
I always check before **SHARING** personal information	
I am **KIND** and polite to everyone	

My trusted adults are:

At school	**At home**

My name is _____ **Year** _____

KS2

These promises help keep me and others safe and happy online, at school and at home.

1. **I use school devices for learning.** I only use the school computers and my school account when my teacher says I can. The school checks what is done on school devices and the school internet, at school and at home.
2. **I ask first.** I only use the websites, apps and games my teacher allows.
3. **I keep my password secret.** I don't share it, even with friends. If someone finds it out, I tell my teacher.
4. **I am careful what I click on.** I don't click on strange links or pop-ups, and I don't download anything without asking.
5. **I am kind online.** I don't send or share unkind or rude messages or pictures. If I see someone being unkind, I tell a trusted adult.
6. **I tell a trusted adult if something worries me.** If I see something upsetting or someone sends me something bad, it is not my fault and I won't be in trouble. I don't share it; I tell a trusted adult straight away.
7. **I keep my private information private.** I don't share my full name, address, phone number, school or photos unless a trusted adult says it is okay.
8. **I know people online may not be who they say they are.** I only talk to people I know in real life. I never meet an online friend without a parent.
9. **I keep my body private online.** I never share photos or videos of myself without checking with a trusted adult. I can say no to dares, challenges or secrets, stop chatting and tell an adult.
10. **I follow age rules.** Apps and games for 13+ or 18+ are not for me.
11. **I respect other people.** I don't change or delete other people's work, and I don't take photos or videos of anyone without permission.
12. **I check what I read.** Not everything online is true. I use the search tools my teacher shows me and ask if I am not sure.
13. **I leave phones and smart watches at home.** If my parents have agreed with the school that I bring one, I leave it on the shelf at the school reception.
14. **I follow these rules at home too.** I tell my parents what I do online so they can help me.

I understand that if I break these rules, I may lose my time on school devices and my parents will be told.

My trusted adults at school are: my class teacher and _____

My trusted adults at home are: _____

I have read and understood this agreement.

Pupil's name: _____ Class: _____ Date: _____

SECONDARY

This agreement is part of the ISO E-Safety and Mobile Devices Policy. It applies in school, on school trips and when I use school accounts at home.

Phones and school devices

1. Phones and smart watches. I hand them in on the shelf at reception when I arrive and collect them at the end of the day. If I don't, my parents may be contacted. If I need to contact my parents during the day, I ask at reception.
2. School devices and accounts. I use them for schoolwork, when a teacher allows. I don't play games unless my teacher gives permission.
3. Monitoring. I know school devices, school accounts and the school internet are monitored, in school and at home. I don't try to get round the filtering (VPNs, hotspots or other people's accounts).
4. Passwords. I keep my passwords private, log out when I finish and never use someone else's account.
5. Searches. I understand staff may search my bag, locker or pockets for devices if there is a reasonable concern, and my parents will be informed.

Behaving safely and responsibly online

6. Photos and videos. I never photograph, film or record anyone without their permission, and never in toilets or changing rooms.
7. Nude or semi-nude images. I never create, ask for, send or forward them, even if someone I know asks. If I receive one, I don't share it; I tell a trusted adult. These cases are always passed to the safeguarding team.
8. Respect. I don't post, send or share anything unkind, threatening or hurtful, including in group chats and outside school. The school deals with this as if it happened in school.
9. My digital footprint. I think before I post, use privacy settings and don't share personal information. What I share online can stay there for ever.
10. Online contact. People online may not be who they say they are. I don't meet anyone I only know online without my parents knowing, and I say no to pressure, dares or requests to keep secrets.
11. Age limits. I follow the age rules for social media, apps and games.
12. AI and honest work. I only use AI tools when my teacher allows it, I say when I have used them, and I don't present other people's work as my own.
13. Speaking up. If I see anything online that worries me, including extremist or violent content, or I think someone is at risk, I tell a trusted adult or the safeguarding team. It is not my fault and I will be listened to.

I understand that if I break this agreement, my phone may be withheld and returned only to my parents, I may lose access to school devices, and sanctions may follow under the Behaviour Policy. Any safeguarding concern will be passed to the safeguarding team.

My trusted adults at school include my form tutor and _____

Student: I have read, discussed and agree to follow this agreement.

Name: _____ Form: _____ Signed: _____

Parent/Carer: I have discussed this with my child. **Signed: _____**

Form tutor: Discussed with the class. **Signed: _____ Date: _____**