Eerde E-Safety Policy

Coordinator:	E-Safety Coordinator
Last reviewed:	Sept 2022
Date for next review:	August 2023

Contents:

Introduction:

We have a duty to provide students with Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills. We believe that used correctly, Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

Eerde, its students and our community exist in a digital world, in addition to this being a valuable resource for education it is also an essential part of living in the modern world. As such, we must equip our students with the skills necessary to be discerning, knowledgeable and safe users of technology in all its forms. The school has limited scope in fully protecting students from access to dangers online outside the school environment, but we can give our students the opportunity to learn themselves what is and is not acceptable, safe and responsible. We need to teach students how to evaluate Internet information, the information they are disclosing, and to take care of their own safety and security in school and beyond.

We have a duty to safeguard children and young people and acknowledge that the online world, with all of its digital communication systems, may present risks to young people. Therefore, we consider e-safety part of our duty to safeguard and promote the welfare of young people. Any cases of improper or dangerous internet use will also be dealt in line with our Safeguarding and Child Protection Policy and any concerns will be reported to the Designated Safeguarding Lead.

Effective E-Safety, which encompasses Internet technologies and electronic communications, will educate students, staff and the Eerde Community about the benefits and risks of using technology and provide safeguards and awareness to enable them to control their online experience.

Aims:

- To make education, rather than software, the most effective tool in maintaining E-Safety;
- To ensure that all Internet users are aware of the risks and the benefits of using the Internet and other technologies to find and share information;
- To provide guidance that students can use to protect themselves outside the classroom;
- To allow reasonable access to the valuable range of educational resources on offer online;
- To ensure that the same values and knowledge are shared by students, staff, and the Eerde community.

Roles and Responsibilities:

Role of the Supervisory Board

The Supervisory Board:

- has delegated to the School Director the appointment of a member of staff as E-Safety Lead, to be responsible for E-Safety;
- has delegated powers and responsibilities to the School Director to ensure all school personnel are aware of and comply with this policy;
- has responsibility for ensuring funding is in place to support this policy;
- has responsibility for ensuring this policy is made available to parents;
- has responsibility for the effective implementation, monitoring and evaluation of this policy
- will annually review all safeguarding policies and procedures.

Role of the School Director

The School Director will:

- ensure the implementation of this policy;
- ensure all school personnel, students and parents are aware of and comply with this policy;
- nominate a member of staff as the E-Safety Lead;
- work with the advice of other organisations and the E-Safety Lead to create a safe ICT learning environment both at school and in boarding accommodation by having in place:
    - an effective range of technological tools
    - clear roles and responsibilities
    - safe procedures
    - education
    - clear boundaries and parameters for the use of technology, personal devices and online resources in class and school;
    - a comprehensive policy for students, staff and parents;
- authorised training for the E-Safety Lead in order to understand E-Safety issues and procedures;
- along with the E-Safety Lead, Academic Director and IT Manager receive and respond to any reports of internet/digital media misuse (see appendix C);
- monitor the effectiveness of this policy;
- meet annually with the IT Manager and E-Safety Lead to review the effectiveness of the policy

Role of the Academic Director

The Academic Director will:

- alongside the School Director, ensure the implementation of this policy;
- ensure all students and teaching staff are aware of and comply with this policy;
- work closely with the E-Safety Lead and IT Manager;
- work with the advice of other organisations and the E-Safety Lead to create a safe ICT learning environment both at school and in boarding accommodation by having in place:
    - an effective range of technological tools
    - clear roles and responsibilities
    - safe procedures
    - education
    - clear boundaries and parameters for the use of technology, personal devices and online resources in class and school;
    - a comprehensive policy for students, staff and parents;

- along with the School Director, E-Safety Lead and IT Manager receive and respond to any reports of internet/digital media misuse (see appendix C);
- support the effective implementation of this policy at all times.

Role of the E-Safety Lead

The E-Safety Lead will:

- work closely with the School Director, Academic Director and IT Manager;
- coordinate regular meetings of the E-Safety Group to share developments, review policy and ensure school-wide participation with this policy;
- ensure the E-Safety Group are made aware of a list of inappropriate access attempts, in order to review filtering provision;
- along with the School Director, Academic Director and IT Manager receive and respond to any reports of internet/digital media misuse (see appendix C);
- receive regular training in order to understand current E-Safety issues and procedures;
- annually review the school's practices and procedures with an aim to improving E-Safety,
- work with the advice of other organisations such as Safer Internet Centre NL, School and Safety Foundation NL and Childnet;
- lead the development of this policy and best practice throughout the school for both staff and students;
- with the Lead Tutor, provide, or facilitate the provision of, education and guidance to students on good E-Safety practice through the curriculum, workshops or visiting speakers;
- ensure an annual E-Safety Awareness Week takes place to promote safe usage of digital media platforms;
- provide education, guidance and support to staff on good practice in E-Safety through guidance information, workshops or visiting speakers;
- provide information to parents on the E-Safety work being done in school, where necessary, via channels such as the parent newsletter;
- ensure that students sign the Eerde IBS Digital Learning & Usage Policy (appendix B) at induction and are made aware of any updates, as and when they arise;
- ensure that all Internet users are kept up-to-date with new dangers, guidance and procedures;
- provide training for staff on induction and when the need arises, ensuring they are also aware of the Staff Acceptable Use Agreement (see appendix 1);
- keep up-to-date with new developments and resources;
- work with school IT Team in safeguarding student and staff access to some material through education;
- review and monitor the policy;
- annually review the policy and practices with the School Director, Academic Director and IT Manager

Role of the IT Manager

The IT Manager will:

- work closely with the E-Safety Coordinator, Academic Director and School Director;
- work with the E-Safety Coordinator, Academic Director and School Director to ensure adequate measures are in place to monitor internet usage and filter/restrict access in both the school and boarding accommodation to inappropriate online content;
- along with the E-Safety Coordinator, Academic Director and School Director receive and respond to any reports of internet/digital media misuse (see appendix C);
- along with the E-Safety Coordinator, ensure that the Eerde IBS Digital Learning & Usage Policy are understood and followed by all in school;
- ensure that an effective range of technological tools exist that promote E-Safety while allowing reasonable access to online resources;
- ensure that new programs will be installed onto the school network or school-owned stand-alone machines by school IT technicians only;
-

Role of the Lead Tutor

The Lead Tutor will:

- work closely with the E-Safety Lead;
- ensure that E-Safety is included in the school tutor programme;
- aid in the development of e-safety education including inviting visiting speakers and delivering workshops where appropriate;
- facilitate the delivery of an annual E-Safety Awareness Week;

Role of the Designated Safeguarding Lead

The Designated Safeguarding Lead will:

- work closely with the E-Safety Lead;
- ensure that all e-safety related safeguarding issues are followed up in line with the Eerde Safeguarding and Child Protection Policy;

Role of the E-Safety Group

The E-Safety Group will be made up of the following:

- School Director
- Academic Director
- E-Safety Lead
- IT Manager
- Boarding and Pastoral Manager
- Lead Tutor

Members of the E-safety Group will assist the E-Safety Lead (or other relevant person, as above) with:

- disseminating e-safety information to staff, parents and students;
- the review and monitoring of the school e-safety policy;
- the review and monitoring of the school and boarding accommodation filtering and monitoring system and requests for filtering changes;
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression;
- monitoring network / internet / incident logs;
- consulting stakeholders – including parents / carers and the students about the e-safety provision.

Role of School Personnel

School personnel will:

- comply with all aspects of this policy;
- undertake appropriate training;
- accept the terms of the Staff Acceptable Use Agreement (appendix 1) before using any Internet resource in school;
- are responsible for promoting and supporting safe behaviours with students and E-Safety procedures;
- will ensure that the use of Internet-derived materials complies with Copyright Law;
- ensure any concerns about e-safety are raised with the Designated Safeguarding Lead and E-Safety Lead;
- ensure all safeguarding concerns are reporting as per the Safeguarding and Child Protection Policy.

Role of Students

Students will be aware of this policy and will be asked to:

- accept the terms of the Eerde IBS Digital Learning & Usage Policy before using any Internet resource in school or accommodation;

- be critically aware of the materials they read;
- validate information before accepting its accuracy;
- acknowledge the source of information used;
- use the Internet for research;
- respect copyright when using Internet material in their own work;
- be aware of the risks of using geo-location tools;
- be aware of the risks of sharing personal information online;
- be aware of the information they share about others;
- be aware of the effect of their 'digital footprint' on university and job applications;
- never take part in any form of online abuse;
- report receiving any offensive communications or online abuse;

Role of Parents/Carers

Parents/carers will:

- be aware of and comply with this policy;
- be asked to support this E-Safety policy and engage with the school when necessary;
- report to the school any concerns they have about their child's use of online resources and digital media.

Role of the Data Protection Officer

The Data Protection Officer will:

- have expert knowledge of data protection law and practices;
- inform the school and school personnel about their obligations to comply with the GDPR and other data protection laws;
- ensure data management is strengthened and unified;
- monitor compliance with the GDPR and other data protection laws, in line with the Eerde IBS Data Protection Policy.

Procedure:
Internet Filtering and Monitoring Systems

We have a contract with a reputed and national Internet provider to manage a secure, monitored and filtered Internet service which enables us to safely access and use the Internet and all email. The Internet filtering service will be annually reviewed.

Access to the Internet is designed to protect students and school personnel by blocking and monitoring attempted access to the following content:

- adult content containing sexually explicit images/ videos
- violent content containing graphically violent images
- hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- illegal drug taking content relating to the use or promotion of illegal drugs or the misuse of prescription drugs
- criminal content relating to the promotion of criminal and other activities
- gambling content relating to the use of online gambling websites
- any content which the school deems unproductive or malicious

All users access the Internet in accordance with the School's Acceptable Internet Use & Agreement and will inform the E-Safety Lead and IT Manager if at any time they find they have accessed inappropriate Internet sites.

When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary the Police.

Educating students about online safety

Eerde students will be taught about online safety as part of the school curriculum, covered mainly by their scheduled weekly tutor sessions and through E-Safety Awareness Week, visiting speakers and/or workshops.

Education provided to **Primary Students** is intended to help them understand:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- How to report concerns and to whom

Education provided to **Secondary Students** is intended to help them understand:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About 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
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- 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 see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- 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

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy and key safety information will be shared with parents via our website.

Online safety may also be covered during parents' evenings, where necessary.

Cyber-bullying

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. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are 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. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed during sessions such as E-Safety Awareness Week and school workshops. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

Key school staff are permitted to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including laptops, mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, staff must:

- Confiscate the device
- ensure that another member of staff is aware that the device is being confiscated and for what reason
- report it to the DSL, DDSL, who will then consult with the Management Team to decide whether they should:
    - Delete that material, or
    - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
    - Report it to the police

Any searching of students will be carried out in line with the school policy on screening, searching and confiscation - found in the school behaviour policy.
Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All students, staff and volunteers (where applicable) are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet - see ***Eerde IBS_Student Digital Learning & Usage Policy and Appendix 1_Staff Acceptable Use Agreement***. Visitors will be 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.
We will monitor the websites visited by students, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

Students using mobile devices in school

Students are not permitted to use their mobile phones or electronic devices during the school day. All electronic devices, other than their school issued laptop, must be kept in lockers or in their boarding accommodation.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.
External storage devices must not be used to store, transfer or move any school data.
If staff have any concerns over the security of their device, they must seek advice from the IT Manager.
Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a student misuses the school's IT devices, systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT devices, systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedure (see HR Policy). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

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 at least once every 2 academic years as part of safeguarding training, as well as relevant updates as required (for example through emails, newsletters and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Student Consultation

We wish to consult our students and to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

Student consultation is integral to our process of regular self-evaluation and continuous improvement and will take place in a variety of ways.

The methods will include:

- A Student Council (which will meet regularly and also be consulted by the Academic Director)
- An appointment system and means of contact with the Academic Director and key staff members
- Operating an 'open door' policy in school whenever possible
- Student Questionnaires (on a variety of matters relating to the school and/or and social issues)
- Open Class discussion (on a variety of matters relating to the school and/or and social issues)

Every effort is made to provide a variety and range of consultation methods to all students. Every student who attends Eerde International Boarding School will be encouraged and given the opportunity to provide feedback on every aspect of school life during their time with us.

A separate policy exists for student consultation which explains these processes in more detail.

Associated Policies and Publications

This policy has been written with reference to and in accordance with the following policies and publications:

- Eerde IBS Safeguarding and Child Protection Policy
- Eerde IBS Anti-Bullying Policy
- Eerde IBS Behaviour and Conduct Policy

Equality Impact Assessment

We are also committed to Articles 2 and 14 of the United Nations Convention on the Rights of the Child and therefore, have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.
Therefore, this policy has been equality impact assessed to ensure that it is fair, it does not prioritise or disadvantage any student and it helps to promote equality at this school.

This policy affects or is likely to affect the following members of the school community (✔)				Students	School Personnel	Parents/ carers	Board	School Visitors	Wider School Community	
				✔	✔	✔		✔		
Question	**Protected Characteristics**								**Conclusion**	
Does or could this policy have a negative impact on any of the following?	Age	Disability	Gender	Gender identity	Pregnancy or maternity	Race	Religion or belief	Sexual orientation	Undertake a full EIA if the answer is 'yes' or 'not sure'	
YES									**Yes**	**No**
NO	✔	✔	✔	✔	✔	✔	✔	✔		✔
UNSURE										
Does or could this policy help promote equality for any of the following?	Age	Disability	Gender	Gender identity	Pregnancy or maternity	Race	Religion or belief	Sexual orientation	Undertake a full EIA if the answer is 'no' or 'not sure'	
YES	✔	✔	✔	✔	✔	✔	✔	✔	**Yes**	**No**
NO									✔	
UNSURE										
Conclusion	We have come to the conclusion that after undertaking an initial equality impact assessment that a full assessment is not required.									

Policy Review

Annual Policy Review Sheet - Appendix A:

Review Date	**Primary Reviewer Name (Policy Coordinator)**

This Appendix A should be completed **annually** by the Policy Coordinator.

Date of Last Review:	
Date of Next Review:	
Is this policy being implemented fully, with all outlined procedures followed as prescribed?	YES/NO
If this policy is not being implemented fully, as prescribed, please outline what you have put in place instead and the reasons behind the change…	
How are staff made aware of this policy?	
Does this policy require any specific/specialised training for staff, if yes please specify what it is and whether it has been done?	
Monitoring the Effectiveness of the Policy **Please comment on the overall effectiveness of this policy – giving any suggestions or recommendations for improvement…**	