German School Association Ltd · Douglas House · Petersham Road · Richmond · TW10 7AH · UK

E-SAFETY POLICY

Title	SR03 – E-Safety Policy
Version	1.8 June 2024
Created	IT
Validity	Pupils, Parents, Staff, Third parties
Next review date	June 2027 or sooner if required

1. Purpose and Scope

We believe that children should be able to use the internet and digital media for education and personal development but that safeguards need to be in place to ensure they are kept safe.

We recognise that technology including use of the internet and online communications can enhance learning and provide social as well as educational benefits. However, new technologies also pose risks categorised in the Statutory Guidance Keeping Children Safe in Education 2023 as online:

- content – being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization, and extremism;
- contact - being subjected to harmful online interaction with other users; for example: 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 - online behaviour that increases the likelihood of, or causes harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images) and online bullying or cyber bullying.
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The purpose of this policy is to ensure:

- that the German School community is aware of the appropriate behaviours which must be followed to safeguard our pupils from these risks;
- the safety and wellbeing of our pupils is paramount when using ICT;
- the School operates in line with our values and within the law in terms of how ICT is used.

We recognise that we have a duty to ensure that all pupils are protected from potential harm online and that all children regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

This policy applies to all members of the School's community including pupils, parents/carers, visitors and staff who have access to and are users of the School's ICT (Information, Communications, Technology) systems, including fixed devices and mobile devices (such as PCs, laptops, mobile phones, webcams, tablets, digital whiteboards and video/video conferencing equipment) owned by the School or brought onto the School's premises. It also applies to use of technology outside of the School's premises which affects the welfare of the School's pupils, is contra to the School's ethos and rules or puts the School's reputation at risk.

In this policy "staff" includes all school staff, employees paid or voluntary as well as contracted third party providers.

2. Linked Policies

This policy should be read alongside the School's policies and procedures including:

Safeguarding Children and Child Protection Policy
Anti-Bullying Policy
Behaviour Policy for Pupils
Disciplinary Policy
Staff Code of Conduct
Staff Social Media Policy
Staff IT Policy
Acceptable use of iPad Policy
Data Protection Policy

Breaches of this policy will be handled in accordance with the procedures outlined in the above policies as appropriate.

3. Technologies

This policy relates to information and communication technology ("ICT") including but not limited to the use of computers, mobile phones, tablets, other electronic equipment and systems to collect, store, use, and send data electronically such as e-mails and web-based and mobile technologies that turn communication into active dialogue ("social media") e.g. blogs, wikis, virtual learning resources, social networking websites, podcasts, forums, message boards or comments on web articles.

The School uses a range of devices including PC's, laptops, tablets, etc. In order to safeguard the student and in order to prevent loss of personal data we employ assistive technology, such as Internet Filtering software that prevents unauthorized access to illegal and inappropriate websites and Email Filtering software that prevents infected email from being sent from the school, or to be received by the school.

4. Roles and Responsibilities

The School has appointed its IT Manager as E-Safety Officer, to coordinate our online safety procedures. In order to be able to fulfil this task, the E-Safety Officer works closely with the School's designated safeguarding lead and liaises with a group of pedagogical staff for purposes of communication and training.

The School's IT department's role includes maintaining a safe ICT infrastructure and keeping up-to-date with technical developments.

Staff will be given appropriate guidance on ICT matters and content and application of this policy.

Pupils and our staff are responsible for their conduct and behaviour online and when using ICT in the same way that they are responsible in circumstances which do not concern ICT. Their use of technology should be in line with all of our linked policies.

We recognise that working in partnership with pupils' parents/carers is essential in promoting children's welfare and supporting them to be responsible in their approach to their use of ICT and

online safety.

This policy is communicated to parents/carers via the School's website. Advice on e-safety is provided to parents/carers from time-to-time at parents' evenings.

Staff are responsible for reporting e-safety incidents to the designated safeguarding lead using the form in Appendix I of this policy.

In incidences where a child has suffered or is at risk of suffering significant harm the School's Safeguarding and Child Protection Policy will be consulted.

5. Rules for e-mail messages

Communication with all those involved in school life should be conducted with mutual respect and openness. This applies to all forms of communication, especially e-mail messages. Initially, all issues and complaints should be discussed among those directly involved.

The purpose of e-mails is the exchange of information. E-mails should not be a medium for discussion, complaints or conflict resolution. The tone of e-mails should be respectful and objective. E-mails should be concise, clear and polite. DSL staff will answer e-mails within a reasonable period during working hours. Information about a pupil's academic standing will not be given via e-mail. Exceptions to this rule must be approved by school management.

If any form of communication sent or received is deemed to be inappropriate and does not comply with our rules of mutual behaviour, this will be passed on the Code of Conduct Team.

6. E-Safety Education for Pupils

E-safety is formally taught at age appropriate levels during ICT lessons and as part of our curriculum following the KMK of Baden Württemberg, where ICT is used in the majority of teaching. Therefore, the School also embeds teaching around e-safety throughout the curriculum. We reinforce e-safety messages throughout learning activities in all subjects and in school assemblies.

During this teaching we ensure that all primary and secondary school pupils are aware of and understand the School's acceptable use requirements below.

7. Use of Technology

In keeping with our mission statement, communication within the School community including online should be conducted with mutual respect and openness.

Offences of a criminal nature, such as hacking, password theft, copying third party software without a license, may lead to prosecution from which the school can not protect any member of the community.

Where pupils' email accounts are provided they are primarily to enable pupils to communicate with peers and school staff and internet access is provided as a resource to support pupils learning.

Kindergarten and pre-school pupils do not have access to ICT/online resources unsupervised.

The class teacher and parent/carer of primary and secondary school pupils must discuss and ensure pupils in their class understand and agree to the following which is based on NSPCC guidance:

1. Only use ICT systems in school, including the Internet, email, digital video, mobile technologies etc. for school purposes.
2. Only use ICT personal equipment which has been authorised for use on the school systems.
3. Not download or install software on school equipment.
4. Protect school ICT equipment form misuse or risk of breaches to confidentially and integrity including keeping equipment safe from damage and theft, using passwords and always logging of after use.
5. Only log onto the school network/learning platform with their own school username and password and not to use other sources of internet e.g. 4G which present risks to the School's network security.
6. Follow the school's ICT security system and not reveal their passwords to anyone and to change them regularly.
7. As far as provided only use their class e-mail address or own school e-mail address for email communication.
8. Make sure that all ICT communications with pupils, teachers and others are responsible and sensible.
9. Understand that they are responsible for their behaviour when using the Internet and that this includes resources they access and language they use in online communications.
10. They will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If they accidentally come across any of this material they will report it immediately to their teacher.
11. Not give out their personal details online e.g. name, phone number or address.
12. Not arrange to meet someone unless it is part of a school project approved by their teacher.
13. Understand that images of pupils and/or staff are only to be taken, stored and used for school purposes in line with school policy and may not be distributed outside the school network without the permission of the Head Teacher.
14. Ensure that their online activity including the use of social media, both in school and outside of school, will not cause the School, staff, pupils or others distress or bring into disrepute.
15. Support the School approach to online safety and not deliberately upload or add any images, video, sound or text that could upset or offend any member of the school community.
16. Respects the privacy and ownership of other's work online at all times.
17. Students are asked not to bring personal devices with their own internet access, such as laptops and tablets, to school. Any efforts to set up your own hotspots or use unauthorized means to gain Internet access during school operations are expressly prohibited.
18. Bypassing the Internet Filtering System or using VPNs not authorized by the school or IT Manager is considered a violation of this policy. Likewise, attempts to gain unauthorized access to the school network or the Internet are unacceptable and will be subject to appropriate action in accordance with the Conduct and Discipline Policy.
19. Understand that their use of the Internet and other ICT can be monitored and logged and

will be made available to their teachers.

20. Understand that these rules are designed to keep them safe and that if they are not followed school sanctions will be applied in line with the school's Behaviour and Discipline Policy and their parent/carer may be contacted.
21. Not physically damaging or otherwise interfering with the facilities, for example adjusting monitor settings and remove keys from the keyboards.

8. Pupils with Special Educational Needs and Disabilities (SEND)

We recognise that pupils with SEND, in particular those with communication and interaction difficulties, have increased vulnerability to online risks.

We make reasonable adjustments to the above education in order to mitigate this vulnerability. Adjustments can be special presettings in grades 5-8, for example with access restrictions. In years 9 to 12, specific arrangements can be made in consultation with parents and the pupil concerned. Parents are welcome to seek support for this from the school's counselling team.

9. Cyber-bullying

Cyber-bullying is behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally which takes place via the of ICT, e.g. e-mail, text messages, social media or gaming, which can include the use of images and video and sexting "youth produced sexual imagery".

Cyber-bullying can occur in or outside of school at any time of day with a potentially bigger audience. The school reserves the right to take action in relation to cyber-bulling which has occurred outside of School.

Incidents of cyber-bullying are managed under the school's Anti-Bullying Policy, in addition to our Behaviour and Discipline Policy and Safeguarding and Child Protection Policy where appropriate.

10. Passwords

- When a person is issued with a school username/password to access our network and resources they must change their password the first time they log on to the account and use a password which meets the following requirements:Minimum of twelve (12) characters in length.
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
- Where possible the use of non-alphabetic characters and numbers (e.g., !, $, #, %, 5) is recommended to have a stronger password.
- Must not be the same as or include the username.
- Passwords must not be easily guessable.
- Mandatory password changes must occur if a password breach is identified, or the user suspects their password may have been compromised.
- Usernames and passwords must not be shared, written down or stored in easily accessible areas.
- Do not use the same password for DSL accounts as for other non-DSL access (e.g., personal email, social media, etc).

11. School e-safety measures

The school provides a secure and positive learning environment for students, both inside and outside the classroom. The school has implemented several measures to keep the students safe:

- **Content filtering and security**: The school uses a content filter solution with advanced security software on the computers and students' iPads, designed to enhance safety and security without invading privacy inside and outside of the school. It applies safe search on all browsers, filters potentially harmful online content, and protects against security threats.

- **Streamlined app access**: To maintain a focused learning environment, the App Store on student iPads is restricted. This allows the school to control the apps available for educational purposes.

- **Supervised Chats on Microsoft Teams**: to support safe and controlled communication within the learning environment through a secure platform like Microsoft Teams the school applies supervised chats. This helps ensure students can interact safely and responsibly online.

- **Classroom management**:
  The school provides access to the Apple Classroom and Jamf Teacher apps, to empower teachers to enhance classroom effectiveness and improve the learning environment. Utilizing these apps allows teachers to manage and monitor student device screens, control access to specific apps, streamline lesson delivery, and facilitate interactive learning activities. These functionalities foster a focused learning atmosphere, enable personalized support, and encourage student collaboration.

- **Security talks**:
  The school provides security workshops to parents/carers and students to empower them by providing valuable insights into online safety practices and promoting responsible digital citizenship; enabling them to make informed decisions and foster a safe online environment both at school and at home.

Appendix I

DEUTSCHE SCHULE LONDON

E-safety Incident Reporting Form

Your details		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home:		
Who was involved in the incident? Child/young person ☐ Name of child……. Staff member/ volunteer ☐ Name of staff member/ volunteer…… Other ☐ please specify……		
Description of incident (including IP addresses, relevant user names, devices and programs used)		
Action taken: • Incident reported to designated safeguarding lead • Advice sought from Safeguarding and Social Care • Referral made to Safeguarding and Social Care • Incident reported to police • Incident reported to Internet Watch Foundation • Incident reported to IT • Disciplinary action to be taken • E-safety policy to be reviewed/amended ☐Other (please specify) ……..		
Outcome of investigation:		