The British Junior Academy of Brussels
e-Safety Policy
This policy applies to the whole school including Early Years

1.0 INTRODUCTION AND SCOPE

This policy seeks to formalise the management of e-Safety risks, incidents, and education within the school. It should be read in conjunction with the school Safeguarding Policy, the staff Code of Conduct, Acceptable Use Policy, school Privacy Statement and the Anti-Bullying Policy. These detail the steps that should be taken in any safeguarding issue whether it is mediated by technology or not.

While many of the risks around e-Safety will be familiar, modern technologies have created a landscape of challenges and dangers that are still constantly changing. The continued development of systems and devices means that school leaders will need to be proactive and pragmatic in dealing with problems and threats as they emerge.

This e-Safety Policy applies to all members of the school community including staff, students/pupils, volunteers, parents/carers, and visitors. It applies to the whole school, including the Early Years Foundation Stage.

2.0 THE NATURE OF E-SAFETY AND BJAB PROVISION

Internet access is a feature of everyday life both in and out of school. Pupils and staff may use a number of networks and a range of devices in a single day and each may have different levels of access and capability. We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks. This means some children, whilst at school, may use mobile phones and smart technology inappropriately.

The British Junior Academy of Brussels believes that schools should be safe environments for learning. We judge the safeguarding of pupils both inside and outside school to be of the highest priority and therefore we adhere to the following principles:

- The highest standards of technological protection are included as part of school networks by regularly setting restrictions on iPads used by children.
- Pupils are taught about e-Safety in all its aspects as part of the curriculum, and e-safeguarding is seen as a responsibility of all staff.
- The school regards e-Safety education as an important preparation for life.
- The school recognises that pupil and family information is sensitive and private. Data protection is regarded as a high priority.

3.0 SYSTEMS AND PROCEDURES

3.1 School Procedures and responsibilities

The school will identify a member of staff to co-ordinate e-Safety. This will be the Debra Johnson. However, e-Safety is seen as a whole-school issue, and different members of staff will have responsibilities as listed below:

Francis Retter **Headteacher**	• Has overall responsibility for e-Safety provision. • Has overall responsibility for data and data security. • Ensures that the school uses a filtered Internet Service. • Ensures that staff receive suitable training to carry out their e-Safety roles and to train other colleagues, as relevant. • Is aware of the procedures to be followed in the event of a serious e-Safety incident.

	• Oversees the staff Acceptable Use (Code of Conduct) arrangements and takes appropriate action over staff who breach them.
SLT	• Takes day to day responsibility for e-Safety issues and assumes a leading role in establishing and reviewing the school e-Safety policies/documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-Safety education is embedded across the curriculum. • Liaises with school IT technical staff. • Facilitates training and advice for all staff. • Is the main point of contact for pupils, staff, volunteers and parents who have e-Safety concerns. • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident. • Ensures that an e-Safety incident log is kept up to date. • Communicates regularly with SLT to discuss current issues, review incident logs and filtering. • Liaises with relevant agencies. • Leads online safety group • Ensures that staff and pupils are regularly updated in e-Safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): o sharing of personal data o access to illegal/inappropriate materials o inappropriate on-line contact with adults/strangers o cyber-bullying.
TopWare Systems (Drives) **Van Roey (Network)** **Network manager/technician**	• Reports any e-Safety related issues that arise, to the e-Safety coordinator. • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Ensures that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • Ensures the security of the school ICT system. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Keeps up to date with the school's e-Safety policy and technical information in order to carry out the e-Safety role effectively and to inform and update others as relevant. • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keeps an up to date record of those granted access to school systems.
Data Manager	• Ensures that the school is compliant with all statutory requirements surrounding the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the Data Protection Act 1998. • Ensures that policies on the handling of information are implemented.
Teachers	• Embed e-Safety issues in all aspects of the curriculum and other school activities. • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant). • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• Read, understand and help to promote the school's e-Safety policies and guidance. • Are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use., and implement current school policies with regard to these devices.

	• Report any suspected misuse or problem to the e-Safety coordinator. • Maintain an awareness of current e-Safety issues and guidance, e.g. through CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff Code of Conduct.

3.2 Filtering protection, AUA confirmation, and monitoring

BJAB is centrally provided with its data connections via a dedicated network. The filtering prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to educational material from (for example) YouTube.

A copy of the Acceptable Use Agreement is within the Staff Handbook which all staff are given access to at the start of their employment. They have a dedicated log-on which requires them to use a strong password for access to the system.

Visitors to the school can be given access to the Internet by connecting to Visitor wireless. Access is only provided if the visitor signs a disclaimer which outlines restrictions and expectations of use.

System monitoring is undertaken on a needs basis. Likewise, where needed, reports can be generated through TopWare Systems about the types of sites being accessed by users of the system.

The e-Safety Coordinator keeps a log of all e-Safety incidents in the school and shares this on a regular basis with the senior leadership team and school network manager. She also monitors the implementation of the e-Safety Policy and ensures that its provisions are being implemented.

3.3 Guidance for users of school systems

The Acceptable Use Agreement for staff details how school equipment and connections may be used.

Pupils receive e-Safety guidance in the form of age-appropriate leaflets, posters, and class lessons. Although not a legal contract, this guidance sets out what is expected by the school.

Access for visitors is provided under the general terms and conditions of BJAB, which prohibit the sending or receiving of materials which "are offensive, abusive, defamatory, obscene, or menacing" or which are illegal.

3.4 Authorising internet access

All staff are familiar with the IT Acceptable Use Policy.

The school will keep a record of all staff who are granted Internet access through the individual usernames granted. The record will be kept up-to-date. (This will take account of changes such as a member of staff who has left the school.)

3.5 Staff use of Equipment and the Internet

The equipment provided for staff is primarily intended to support the teaching and learning of pupils. However, it is unreasonable to deny staff access to the Internet for legitimate personal use (for example to contact a son's or daughter's school). Nevertheless, discretion and the highest professional standards are expected of staff using school equipment.

Expectations are set out in detail in the Acceptable Use Agreement and in the Code of Conduct, but will include:

- Keeping a proper professional distance e. g. not "friending" pupils on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or e-mails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents.

3.6 Misuse of school systems

Pupil misuse (for example the sending of bullying messages to another pupil) may result in the withdrawal of facilities or further sanctions in line with the school's behaviour policy.

Abuse of the systems by visitors will result in the immediate withdrawal of access and possible further action depending on the nature of the misuse.

4.0 E-SAFETY, PUPILS AND SAFEGUARDING

4.1 Guidance to pupils on using e-mail and other messaging systems

Pupils are advised never to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

Pupils are advised never to send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students are reminded that the sending of abusive messages is illegal.

4.2 Teaching e-Safety in School

The school curriculum includes lessons and activities in e-Safety for all pupils.

The intention is to develop pupils' awareness, resilience, and skills in the wider electronic world. Pupils will explore issues such as:

- Persuasion and reliability (internet scams, phishing, unreliable information, radicalisation and extremism, etc.);
- Personal information and safety (sexting, social network information, personal images, etc.);
- Online bullying (text abuse, "trolling", etc.).

The activities are differentiated with regard to age.

The curriculum is varied and may comprise:

- staff-led skills sessions (e.g. How to safe search on the internet)
- whole-school assemblies and other examples of peer mentoring
- discussion groups
- e-Safety week (as part of Healthy Week)
- formal lessons.

The teaching covers not only what the problems are, but how to deal with and avoid them. These activities and lessons form part of the Computing scheme of work.

The e-Safety Coordinator and DSL keep up to date on emerging trends and alters the guidance and focus of the curriculum appropriately.

4.3 Staff training and updates

- All staff are aware of the IT Acceptable Use policy, which is referenced in the Staff Handbook
- All staff receive regular training in safeguarding pupils. e-Safety is included as part of this. Staff members receive a broader update at least once a year.
- e-Safety incidents and concerns are raised at SLT and staff meetings.

4.4 Reporting of e-Safety concerns

The school takes reports concerning e-Safety very seriously. The action taken depends on the nature of the concern raised.

All incidents that come to the attention of school staff should be notified to the e-Safety Coordinator and DSL via CPOMS.

The e-Safety Coordinator will ensure that pupils, parents, volunteers, and staff understand that they can contact them with concerns at any time.

Any incident that raises wider safeguarding questions will also be communicated to the Designated Safeguarding Lead and action under the Safeguarding Policy will be considered.

4.5 Particular concerns:

Inappropriate material appearing on school computers

- Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting. They are encouraged to talk to their teacher. The teacher should report the incident to the e-Safety Coordinator who will log the problem and liaise with the network manager to adjust filtering settings.

Abusive messages on school computers

- Pupils who receive abusive messages will be supported. The e-Safety Coordinator will be informed and an investigation begun initially with the help of the Network Manager.

Parental reporting of bullying/pressure

- Parents may become aware that their child is suffering from bullying or other pressures originating in the school but continued via electronic means. Parents should know that the school encourages parents and pupils to approach them for help, either via the class teacher or directly to the Head. A full discussion of Cyber bullying, and the actions which may be taken, can be found in the Anti-Bullying Policy.

Pupil disclosure of concerns or abuse

- For many reasons, a pupil may choose to disclose a concern to a member of school staff. The situations leading to a disclosure can range widely, from a general worry to long-term abuse, and for this reason safeguarding training for all staff is conducted so that situations or concerns are dealt with appropriately. A disclosure should always follow school procedure be passed on to the Designated Safeguarding Lead.

Pupil reporting outside school

- Pupils are taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with their parents, and consider using the Report Abuse button to make a report and ask for help.

5.0 RISK MANAGEMENT – EVERYDAY E-SAFETY

5.1 Assessing risks

The school will take all reasonable precautions to ensure that users abide by the acceptable use rules and access only appropriate material.

The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use rules which are published for their protection.

Due to the international scale and linked nature of Internet content, it is also not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

The school cannot accept liability for material accessed, or any consequences of Internet access.

5.2 Publishing staff & pupil information and photographs

- **The school website**

The contact details on the website should be the school address, email and telephone number. Pupils' personal information will not be published.

- **Publishing pupils' images and work on the web**
    - **Open / public sites**

Public sites could potentially be used to gather information and the locations of pupils. Written permission to publish photographs is obtained on a case-by-case basis by parents.

5.3 Using web sites with pupils

Pupils are often directed to Internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing digital world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- If pupils are asked to make online accounts for access to materials, the minimum of identifiable personal information will be disclosed and only school emails will be used.
- The school will be as open as possible about the sites and software it uses, and it welcomes queries from parents who wish to raise concerns or understand more about the way that IT contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions which do not apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

5.4 Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risks will be assessed. It should be understood that potential problems or harm may not emerge until after the adoption of a technology.

The Senior Leadership Team of the school (including the e-Safety Coordinator) will reassess the suitability of technology and systems over time and check that they remain suitable, secure and effective.

5.5 Handling e-Safety complaints

Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the procedures of the school and according to the nature of the complaint.

Any complaint about staff misuse must be referred to the Head. If the complaint is about the Head, it should be referred to the Proprietor.

Complaints of a child protection nature must be dealt with in accordance with statutory child protection procedures and the school's safeguarding policy.

Pupils and parents are informed of the school's complaints procedure, which is available on the school website.

5.6 Using Non-School technology

We recognise that students in the Upper School may carry mobile technology to school for use when travelling to and from school. All mobile technology should be placed on flight mode upon entering the building and remain in their lockers during school hours. Pupils in Lower School are not permitted to bring mobile technology to school.

Under some circumstances, teachers are now able to use their own equipment in school and connect to the available network. This is normally called "bring your own device" (BYOD); students from Year 10 may also do so but may only connect to the student wifi network.

It is made clear to the member of staff that the rules and expectations surrounding online behaviour remain in force regardless of the ownership of the equipment being used.

6.0 COMMUNICATING THE POLICY

6.1 Introducing the e-Safety policy to children

- Versions of the e-Safety Use rules are posted in all classrooms and discussed with pupils as needed. The aim is to keep the policy familiar and fresh for pupils rather than treated as something which is only referred to at odd times.

- Pupils are made aware that network and Internet use is monitored.

6.2 Staff and the e-Safety policy

- All staff will be given a copy of the e-Safety Policy and Acceptable Use Agreement. Their importance will be explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Because of this, discretion and professional conduct are essential.

6.3 Communicating e-Safety information to parents

- The school website gives information on e-Safety and how the school can help.
- The school holds e-Safety events to brief parents about e-Safety developments and policies; possibly as part of events such as 'Healthy Week.'

7.0 MONITORING AND REVIEW

This policy is the responsibility of Mr Retter, the Headteacher and Madame De Maertelaere, the Proprietor.

Headteacher: .... (Francis Retter) **School Proprietor ………………………………….……………. (Madame De Maertelaere)**	
Updated: May 2025	**To be reviewed:** May 2026