

École Française de Bristol



E-Safety Policy

Last review date:	February 2024
Next review date:	February 2026

Rationale

The Internet and other digital technologies permeate all aspects of life in a modern technological society. The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management of information and business administration systems. Ensuring that the Internet is used safely and appropriately is a key requirement for all schools, as well as teaching children to be safe outside of school.

This policy applies to all pupils, all teaching staff, all support staff, all members of the committee, directors, all volunteers and anyone on work experience at the École Française de Bristol.

Aims of the policy:

Our aims are to ensure that all pupils:

- will use the Internet and other digital technologies appropriately and safely to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the Internet;
- will develop a positive attitude to the Internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Pupils will be taught:

- about the safe use of the Internet;
- about what to do if they encounter a problem online and how to report abuse;
- how to use the Internet safely in various situations in and outside school.

General Network Security

The École Française de Bristol uses a filtering system – currently Open DNS – which is designed to filter out material found to be inappropriate for use in the education environment.

Use of the Internet

- Pupils should only access the Internet during lesson time. Internet use will be supervised and monitored at all times. For younger pupils up to Y2, this means an adult directly supervising. For Y3, 4, 5 and 6 an adult will be responsible for monitoring pupil's use at regular intervals (generally at least every 10 minutes);
- Pupils will only be allowed to send emails and messages as part of a curriculum activity that is supervised by the teacher;
- Pupils must not reveal personal details of themselves or others in any online communication, or arrange to meet anyone;
- If staff or pupils discover **unsuitable sites**, it must be reported to the Headteacher **immediately**. An incident form will be completed: the URL (website address) and content of the website must be reported on the form. Illegal sites will be reported to the Internet Watch Foundation at iwf.org.uk.

In the following cases the monitoring should be referred to the **Police immediately**:

- o incidents of 'grooming' behaviour
- o the sending of obscene materials to a child
- o adult material which potentially breaches the Obscene Publications Act
- o criminally racist material
- o promotion of terrorism or extremism
- If offensive, threatening or bullying emails or messages are received, pupils must immediately tell the teacher. A complaint must be reported to the Headteacher. The complaint should then be logged in writing. This must include a copy of the offensive email, full headers, dates and times;
- Children are not permitted to use mobile phones in school and in lessons;

- Staff and pupils must ensure that materials derived from the Internet comply with copyright law;
- Everyone must be polite and considerate online and report any issues that are likely to cause offense.

Social networking and personal publishing

- Pupils are not allowed access to open social networking sites;
- Although pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, pupils will be taught about the potential risks of social networking sites and what information should not be shared on such sites. The purpose of this is to acknowledge (although not condoning) the reality that some children may already have access to social networking sites.

Use of digital and video images

- Staff should only use school equipment to take digital / video images. The images must be appropriate and support educational aims;
- Staff must follow the school rules concerning the sharing, distribution and publication of those images;
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Written permission from parents / carers must be obtained before photographs are published on the school website.

Terrorist and extremist material

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

- We will ensure that pupils are always under supervision when online.
- Internet safety is integral to our IT curriculum, and we will provide training for our staff and learners where appropriate.
- We are aware of the increased risk of online radicalisation, as extremist and terrorist organisations seek to radicalise young people using social media and the internet. We will try and help our pupils to keep safe online and consider the impact of social media networking sites with additional consideration to the threat of exposure to extremism and radicalisation.
- We will work in accordance with the guidelines around monitoring and auditing staff and learner usage of the internet when in School.

Managing videoconferencing

Videoconferencing will be appropriately supervised for the pupils' age. Parents must have given permission in writing for their child to take part.

Staff use

The use of the Internet on school premises should principally be for school use. This includes such activities as:

- Accessing teacher resources
- Accessing Educational websites
- Researching topics/websites for use with a class
- Use of e-mail for school business

Use of the Internet for non-school purposes is allowed, on the provision that it does not detract from the teacher's job. This includes being adequately prepared for lessons. A breach of this rule would potentially be considered a disciplinary offence.

The use of the Internet to access any pornographic or otherwise illegal sites is a disciplinary offence and will result in police involvement. The school expects all users to use the Internet responsibly and strictly according to the following conditions:

Users shall not: Visit Internet sites, make post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

- Pornography (including child pornography)
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information that may be offensive to colleagues

Any of these offences will be reported directly to the police.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be given to the Headteacher or the Deputies as the need arises;
- Complaints about misuse of the Internet in school by pupils must follow the school's relevant policy (Behaviour, Bullying, Health and Safety).

How will staff, parents and pupils be informed?

- All staff, including supply staff, classroom assistants, pupils, support staff, volunteers, work experience students and directors will have access to the E-Safety Policy, and its importance explained;
- E-Safety rules are posted in each room where a computer / tablets are being used;
- Pupils will be informed that Internet use will be monitored;
- Parents' attention will be drawn to the school E-Safety Policy in newsletters and on the school website;
- All parents will receive support information on issues such as safe Internet use.

Viruses and Spam

All computers have the Microsoft Security Essentials protection.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

Monitoring & Review

- The safety settings of the school computers and tablets will be checked once a year.
- This policy will be reviewed annually.

The use of the school's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body.

Additional resources

- NSPCC
nspcc.org.uk/keeping-children-safe/online-safety - Organisation which provides a whole range of resources on online safety
- Think U Know
www.thinkuknow.co.uk - Home Office site for pupils and parents explaining internet dangers and how to stay in control
- Childnet
www.childnet.com - Guidance for parents, schools and pupils
- Kidscape
www.kidscape.org.uk/resources

- Internet Watch Foundation
www.iwf.org.uk - Invites users to report illegal websites
- South West Grid for Learning
www.swgfl.org.uk/safe - A comprehensive overview of web-based resources to support schools, parents and pupils