

Online safety policy

The purpose of this policy is to safeguard and protect all our young people and staff when using the internet and other online technologies. The document specifies the expectations for all key stakeholders and is supplemented by additional documentation available on the school directory.

Managing Risks

The main risks to the school encompass inappropriate content, hate sites, cyber-bullying, grooming, sexual content, the prevent duty including: extremism and radicalisation, identity theft and privacy, breach of copyright and reputational damage to the school and its stakeholders.

There are three core ways to mitigate risks to consider, these are:

- Use of technology
- Policies and practices
- Education and training.

The school manages these risks through internet content filtering; secure filtered and anti-spammed email services; protecting personal data; anonymised student email; managed internet content; restricted access to social media; educating young people; staffing and parents and carers training; use of permissions for images and videos; additional access control to networks; effective and timely reporting of issues; effective supervision of use of IT within the curriculum; weekly web access reporting and managing emerging technologies.

Expectations of staff

All staff members are responsible for ensuring they have read and understood this policy and how it is applied in the workplace. Any staff have a duty to report any online safety concerns to either the Data Manager (David Clegg) or alternatively if a safeguarding concern with the schools designated safeguarding leads (Jim Connolly, Tara Gray). All staff are accountable for ensuring that young people and other key stakeholders are safeguarded at all times when online. Young people should be supervised in accessing and using information technology.

Staff must not access inappropriate materials at school or whilst at work, whether this using school owned or personal devices. Doing so will lead to disciplinary action being taken.

Expectations of children and young people

Safe and secure access to IT is important for all our young people. The school encourages all young people to report anything that they see or hear online that they find upsetting or makes them feel unsafe. All young people should be careful not to post any personal information, images, video or audio online unless they have discussed this with a member of staff beforehand.

Expectations of parents and carers

The school expects all parents and carers to support the school in promoting online safety and in enabling the school to safeguard all its stakeholders. The school provides advice and guidance on its website. Parents and carers are welcome to contact the school if they need any help or advice in supporting the safe use of IT and online safety.

Expectations of visitors and contractors

Visitors and contractors may be permitted to use the school Wi-Fi, in doing so they are required to adhere to local rules and procedures and to follow the guidelines outlined in this policy. On occasions visitors or contractors may require the use of school equipment when on site, in these instances you will be required to sign *the ICT acceptable use form* beforehand.

Managing online safety concerns

All online access is filtered and every effort is made to prevent inappropriate materials from being accessible. Owing to the size and complexity of the internet, the school and its internet services providers are unable to guarantee complete filtering. The school maintains the right to monitor all internet access and online activity and may take appropriate action.

Incidents are managed locally by members of SMT and are reportable as safeguarding concerns.

Key stakeholders are provided with training, advice and guidance as to the safe and effective use of online resources on a continual basis. The school is open to suggestions for development opportunities from all groups.

Use of portable devices

Online safety policy and local rules around digital devices apply equally to mobile/portable devices (i.e. Laptops, mobile phones, tablets, hand held devices). All portable devices used within the school are covered by this policy irrespective of ownership.

Use of games consoles

Most games consoles are able to access online content. To help ensure adequate levels of online safety, some consoles used in the school may have online access (Wi-Fi) restricted as deemed appropriate on a person-by-person basis.

Interactive online games may be played where there is adequate supervision available and where the game rating is suitable for the individual.

Online safety as a rights respecting school

As a UNICEF Level 1 Rights Respecting School, Bradstow promotes the United Nations Convention on the Rights of the Child which the UK Government has signed and ensures that the whole school community learns about their rights and show respect for each other.



Article 13 Children have the right to get and to share information, as long as the information is not damaging to them or to others.

Article 29 Education should develop each child's personality and talents to the full. It should encourage children to respect their parents, and their own and other cultures.

Refer also to the following: Acceptable use policy; Safeguarding / child protection policy; ICT social media policy; Prevent duty risk assessment; Online safety risk assessment; Online safety info on our website: <http://www.bradstow.wandsworth.sch.uk/schoolfacilities/onlinesafety.html>

For internal use only:

Policy last reviewed: Oct 2017

Policy reviewed by: Jim Connolly /
David Clegg

SLT responsibility: School Business Manager

Approved by Board of Governors: