living and learning together

BRADSTOW SCHOOL

within a Culture of Gentleness

Online Safety Policy

3 year review cycle. Date for Review: March 2022

For internal use only:			
Policy last reviewed:	March 2019	Policy reviewed by:	David Clegg
SLT responsibility:	School Business Manager	Approved by Board of Governors:	
Approval required from:	Processes, products & Services SC	Requirement:	Non-Statutory

Introduction

The purpose of this policy is to safeguard and protect all our young people (YP) 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, violet imagery, grooming, sexual content, sites that promote negative body image, fake news/radical views, 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 ; Impero network monitoring software; restrictions on digital devices; record of young people devices (including MAC address); risk assessment for specific YP; dedicated classroom devices; guest Wi-Fi sign in; secure filtered and anti-spammed email services; protecting personal data; anonymised children and young people email; managed internet content; restricted access to social media; educating young people including 1-2-1 with a specialist; 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 process (see flowchart below) 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.

Staff that have elevated internet privileges must not allow YP to access the internet with their credentials, e.g. YouTube access, etc.

All staff have a duty to report any online safety concerns to either the Data Manager (David Clegg), ICT Technician (Mark Yorke) or alternatively if a safeguarding concern with the schools designated safeguarding leads. All staff are accountable for ensuring that young people and other key stakeholders are safeguarded at all times when online. YP should be supervised in accessing and using information technology.

Staff must not access inappropriate materials at school or whilst at work, whether using school owned or personal devices. Doing so will lead to disciplinary action being taken. Please also refer to the staff mobile phone policy.

Expectations Of Children And Young People

Safe and secure access to IT is important for all our young people. YP learn about online safety as part of their curriculum. 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. The school provides regular workshops for parents and carers to attend covering online safety. 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 policy* 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. Games consoles are used in communal areas to ensure adequate supervision.

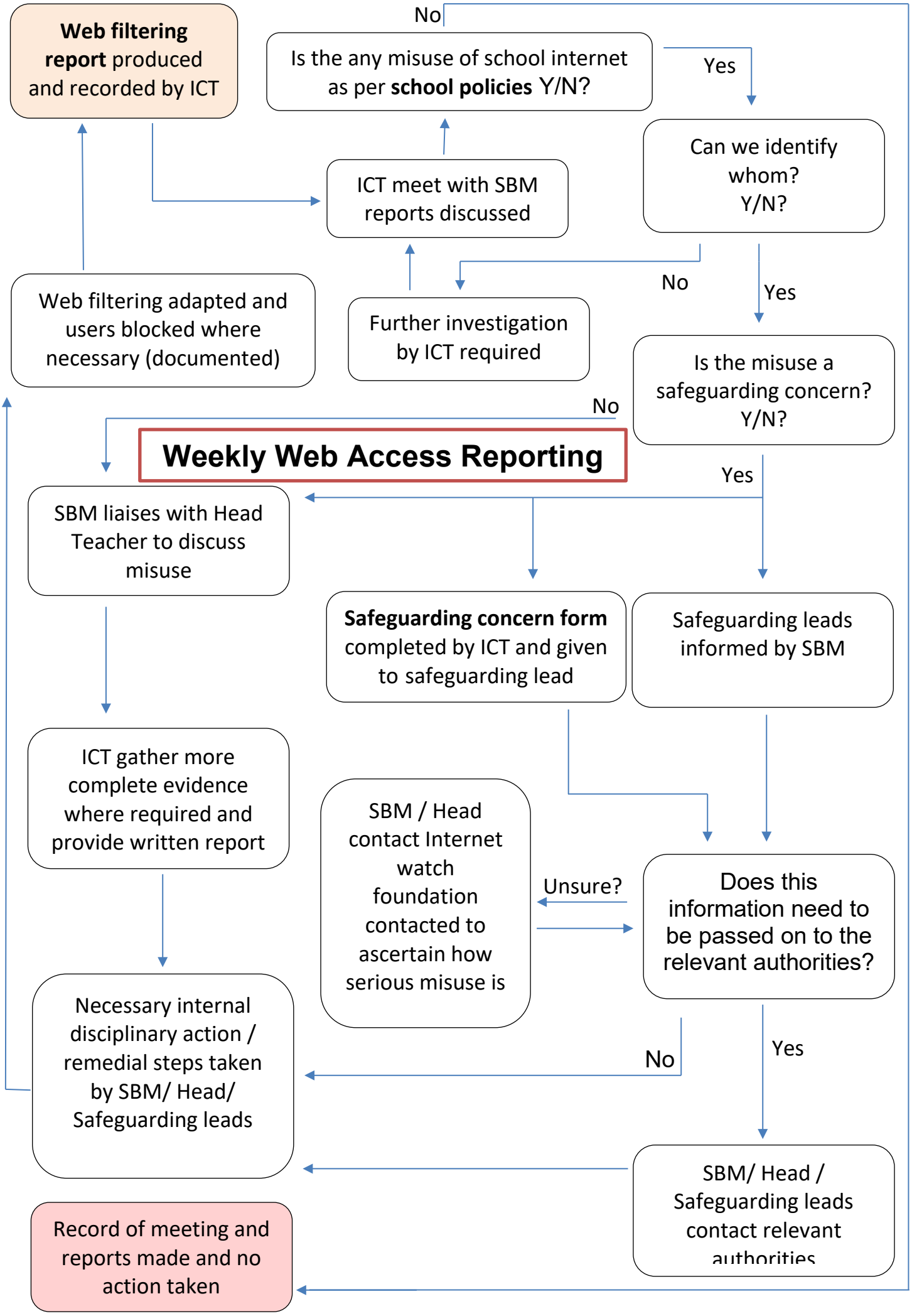
Interactive online games may be played where there is adequate supervision available and where the game rating is suitable for the individual. 18+ games/content is banned and age restrictions and suitability are used within the school.

Online Safety As A Rights Respecting School

As a UNICEF Gold level: Rights Respecting accredited 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:
http://www.bradstow.wandsworth.sch.uk/schoolfacilities/onlinesafety.html


Web filtering report produced and recorded by ICT
No
Is the any misuse of school internet as per school policies Y/N?
Yes
Can we identify whom? Y/N?
ICT meet with SBM reports discussed
Web filtering adapted and users blocked where necessary (documented)
Further investigation by ICT required
No
Yes
Is the misuse a safeguarding concern? Y/N?
No
Weekly Web Access Reporting
Yes
SBM liaises with Head Teacher to discuss misuse
Safeguarding concern form completed by ICT and given to safeguarding lead
Safeguarding leads informed by SBM
ICT gather more complete evidence where required and provide written report
SBM / Head contact Internet watch foundation contacted to ascertain how serious misuse is
Unsure?
Does this information need to be passed on to the relevant authorities?
Necessary internal disciplinary action / remedial steps taken by SBM/ Head/ Safeguarding leads
No
Yes
SBM/ Head / Safeguarding leads contact relevant authorities
Record of meeting and reports made and no action taken

Online Safety Risk Assessment

No	Hazard (danger)	Risk (what could happen)	Individuals Affected	Control measures currently in place
1	**Content (where the YP receives)** Exposure to inappropriate content, such as online pornography, shocking or violent imagery, profanity, tasteless or illegal content Ignoring age ratings in games	Exposure to inappropriate content Potential exposure to content not suitable to age group, including violence, profanity, sexual content and discrimination	YP	1. Web filtering for school devices and wifi attached devices 2. Use of Impero network monitoring software 3. Weekly web report by IT discussed with SBM 4. YP are supervised 5. Online safety covered within the curriculum 6. Suitable alternative games and/or platforms offered 7. Games are installed by ICT team and checks done on age ratings 8. Content control on digital devices
2	**Content (where the YP receives)** substance abuse Lifestyle websites, e.g. pro-anorexia/self-harm/suicide sites	Exposure to inappropriate content leading to unhealthy habits, harmful behaviours Being influenced to self-harm and actually doing this	YP	1. Web filtering for school devices and wifi attached devices 2. Use of Impero network monitoring software 3. Weekly web report by IT discussed with SBM 4. YP are supervised during internet access
3	**Content (where the YP receives)** **Contact (where the YP participates)** Radicalisation, Extremism, violent or hateful content **Conduct (where the YP acts or behaves)** terrorism	Exposure to inappropriate content, promoting unhealthy views/values, etc Leading to potential radicalisation of the YP Commits acts of terrorism as a result of being persuaded by others/what they see online	YP YP, others affected by terrorism	1. Web filtering for school devices and wifi attached devices 2. Use of Impero network monitoring software 3. Weekly web report by IT discussed with SBM 4. YP are supervised during internet access. 5. Annual training for staff: Safeguarding children in education and child sexual exploitation. 6. Safeguarding /Child Protection policy. 7. SMSC curriculum
4	**Content (where the YP receives)** Content validation: how to check authenticity and accuracy of online content, misleading info or advice bias	Exposure to misleading info or advice Being unduly influenced by one set of opinion and not seeing the whole picture before coming to your own view/perspective	YP	1. Online safety training/curriculum YP 2. Safety posters around the school 3. YP are supervised during internet access 4. Safety posters around the school 5. YP are supervised during internet access

No	Hazard (danger)	Risk (what could happen)	Individuals Affected	Control measures currently in place
5	**Content (where the YP receives)** spam	A nuisance / time waste. Potentially containing malicious content Personal info may be given away by YP which may result in identity theft and fraud	YP	1. Spam filters provided by our service provider (LGFL/Atomwide) 2. YP email address is anonymised and domain does not expose geographic location 3. LondonMail used by children and YP and is accessible for monitoring https://www.lgfl.net/services/london-mail
6	**Contact (where the YP participates)** Grooming Meeting strangers	Potentially leading to harm from others, CSE, etc Meet people online or in person who may not be who they claim to be	YP	1. Online safety training YP / curriculum 2. Safety posters around the school 3. YP are supervised during internet access 4. Annual training for staff: Safeguarding children in education and child sexual exploitation 5. LondonMail used by YP and is accessible for monitoring https://www.lgfl.net/services/london-mail
7	**Contact (where the YP participates)** Cyber-bullying in all forms Harassed or stalked on-line **Conduct (where the YP acts or behaves)** Bullying or harassing another/others Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecency images)	Bullying, intimidation, Sexting Causing hurt and distress to others and self Emotional and sexual abuse could impact mental health, damage self-esteem, reputational damage	YP and those being targeted YP, whole school reputation	1. Online safety training YP / curriculum 2. Safety posters around the school 3. YP are supervised during internet access 4. Annual training for staff: Safeguarding children in education and child sexual exploitation 5. LondonMail used by YP and is accessible for monitoring https://www.lgfl.net/services/london-mail

No	Hazard (danger)	Risk (what could happen)	Individuals Affected	Control measures currently in place
8	**Contact (where the YP participates)** identity theft (including 'frape'(hacking Facebook profiles)) and sharing passwords **Conduct (where the YP acts or behaves)** hacking	Identity theft / fraud Reputation damage/embarrassment could impact mental health, damage self-esteem Potentially leading to fine or imprisonment / reputational damage Potential data leakage leading to harm to others	YP YP, damage to organisation being hacked	1. Online safety training YP / curriculum 2. Safety posters around the school 3. YP are supervised during internet access. 4. Internet access guarded by firewall managed/configured by our service provider (LGFL/Atomwide). 5. Server Data backed up daily 6. Use of unshared passwords for network resource access. 7. GDPR policies to ensure data is secure. 8. Acceptable Use policy / Information e-security management policy
9	**Contact (where the YP participates)** Personal info	Giving away personal information to people who may not have good intentions	YP	1. Online safety training YP / curriculum 2. Safety posters around the school 3. YP are supervised during internet access. 4. Annual training for staff: Safeguarding children in education and child sexual exploitation. 5. LondonMail used by YP and is accessible for monitoring https://www.lgfl.net/services/london-mail
10	**Contact (where the YP participates)** Unwelcome persuasions / advertisement. Malware. Pop-ups	Exposure to misleading info or advice	YP	1. Online safety training YP / curriculum 2. Safety posters around the school 3. YP are supervised during internet access
11	**Conduct (where the YP acts or behaves)** Digital footprint and online reputation	Damaging own and/or own reputation Giving away personal information to people who may not have good intentions	YP & whole school	1. Online safety training YP / curriculum 2. Use of Impero network monitoring software 3. Safety posters around the school 4. YP are supervised during internet access. 5. Annual training for staff: Safeguarding children in education and child sexual exploitation. 6. Acceptable use policy, Social media policy

No	Hazard (danger)	Risk (what could happen)	Individuals Affected	Control measures currently in place
12	**Conduct (where the YP acts or behaves)** copyright (little care or consideration for intellectual property and ownership – such as music and film) / illegal downloading	A criminal offence, potentially leading to fine and up to 5 years in prison	YP	1. Web filtering for school devices and wifi attached devices 2. Weekly web report by IT discussed with SBM 3. YP are supervised
13	**Conduct (where the YP acts or behaves)** creating and uploading inappropriate or illegal content	Potentially leading to fine or imprisonment / reputational damage	YP, school	1.Web filtering for school devices and wifi attached devices 2. Use of Impero network monitoring software 3. Weekly web report by IT discussed with SBM 4. YP are supervised / issues reported
14	**Conduct (where the YP acts or behaves)** gambling	Damage to self, family, relationships Financial loss	YP, family, relationships	1. Web filtering for school devices and wifi attached devices 2. Use of Impero network monitoring software 3. Weekly web report by IT discussed with SBM 4. YP are supervised
15	**Conduct (where the YP acts or behaves)** financial scams	Financial loss and associated consequences	YP	1.Web filtering for school devices and wifi attached devices 2. Weekly web report by IT discussed with SBM 3. YP are supervised 4. Spam filtering to try and filter out Phishing attacks
16	**Conduct (where the YP acts or behaves)** Committing online fraud	Potentially leading to fine or imprisonment / reputational damage	YP, school	1.Web filtering for school devices and wifi attached devices 2. Weekly web report by IT discussed with SBM 3. YP are supervised
17	**Computer skills (where the YP acts or behaves)** Use of virtual private network (vpn) to circumvent web filtering, etc	Filtering is rendered ineffective, hence, inappropriate content, etc can be accessed	YP	1. A customised YP agreement is put in place 2. YP are supervised 3. Ongoing reviews
18	**Conduct (where the YP acts or behaves)** Buying questionable/prohibited products (e.g. weapons, intimate apparel, drugs)	Harm to themselves and/or others Potentially leading to fine or imprisonment / reputational damage	YP, staff, school	1.Web filtering for school devices and wifi attached devices 2. Weekly web report by IT discussed with SBM 3. YP are supervised