BJS Federation of Schools

E-Safety Policy

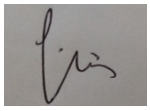
2021

Policy Adopted by Executive Headteacher on: Autumn 2021

Policy Due for Review on: Autumn 2022

Signed _____

Ms A. Parker, Executive Headteacher



Signed _____
Mrs F. Morris, Chair of Full Governing Board

1. Principles

1.1 It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

1.2 This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2. Aims

2.1 Internet access is planned to enrich and extend learning activities. The school has acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies. An E-safety Policy has been drawn up to protect all parties and Rules for Responsible Use of Computing will be discussed with all staff and pupils. All staff members and children will sign the school's Acceptable Use Policy at the beginning of each academic year.

2.2 Although the school offers a safe online environment through filtered internet access provided by London Grid for Learning (LGfL), we recognise the importance of teaching our children about online safety and their responsibilities when using communication technology. This will form part of the children's learning.

3. Curriculum Content and Planning

3.1 Designated lessons on E-Safety are taught at the beginning of each academic year and staff will remind children of different aspects of E-Safety as they use the internet throughout the year. CEOP's (The Child Exploitation and Online Protection Centre) - Think you know website provides different resources for all staff to use to support the teaching and learning of E-Safety, providing different activities for children to work through. The website has films, lesson plans, presentations, practitioner guidance, games and posters, which will be used to teach children how to stay safe. These sessions will empower and protect children from both online and off.

4.Creative Curriculum and Cross Curricular Links

4.1 Internet use will enhance learning

• The school Internet access is designed for pupil use and will include filtering appropriate to the age of pupils.
• Pupils will be taught what Internet use is acceptable and what is not and given clear
guidelines and objectives for Internet use.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
• When appropriate the school will use 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate. The school is vigilant when conducting 'raw' image search with pupils e.g Google search.

4.2 Education programme

At the BJS Federation of Schools we:

• Foster a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable.

• Ensures pupils and staff know what to do if they find inappropriate web material i.e., to switch off monitor and report the URL to the teacher or e-safety co-ordinator

• Pupils are taught how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

• **E-safety** is taught as part of the Computing and PSHE curriculum.

• Ensures pupils and staff know what to do if a cyber-bullying or other e-safety incident occurs.

• Please refer to the live session policy which is used for online learning via Google Classrooms or Google Meets.

4.3 Information system security

At the BJS Federation of Schools we:

• Ensure virus protection will be updated regularly.

• Use class and individual log-ins for pupils. We use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature; Informs staff and pupils that they must report any failure of the filtering systems directly to the subject leader who then informs system administrator. Our systems administrators report to the Headteacher where necessary.

• Block all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.

• Only uses approved blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others.

5. Authorising Internet access

5.1 EMAIL

Pupils may be introduced to and use email as part of the Computing scheme of work. Staff can use the school domain e-mail accounts or web-based email for professional purposes or for uses deemed 'reasonable' by the Head and Governing Board.

5.2 IMAGES

Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication.

• We do not include the full names of pupils in the credits of any published school produced
video materials / DVDs.
• Parents who do not wish for the child to be used in any school produced video or materials can specify this on the acceptable use policy agreement when given at the start of the year.
• Pupils are only able to publish to their own 'safe' web-portal on the LGfL in school.

• Pupils are taught to publish for a wide range of audiences which might include governors,
parents or younger children as part of their Computing scheme of work.
• Pupils are taught about how images can be abused in their E-Safety education Programme.

6. USING THE NETWORK AND EQUIPMENT

At the BJS Federation of Schools we:
• Ensure staff are set-up with Internet and email access and can be given an individual network login username and password.
• Provide pupils with a class network login username.
• Make it clear that staff must keep their login username and password private and must not leave them where others can find them.
• Make clear that pupils should never be allowed to log-on or use teacher and staff logins –these have far less security restrictions and inappropriate use could damage files or the network.
• Make clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles.
• Set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
• Require all users to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then logon again as themselves.
• Request that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
• Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

6.1 Handling Infringements

Whenever a pupil or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management or the Governors in the case of the Headteacher.

6.2 Informing staff and pupils of our procedures.
• They will be fully explained and included within the school's E-Safety / Acceptable Use Policy.

• Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours. Pupils will sign an age-appropriate E -Safety/ acceptable use form.
• The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
• Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.

7. Evaluation and Review

7.1 E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and in compliance with the Policy monitored. The responsibility for E-Safety has been designated to our computing subject leader.

7.2 Our school Child Protection Co-ordinator is The Assistant Headteacher for Inclusion in conjunction with the Computing subject leader. The Computing subject leader and AHT for Inclusion ensures they keep up to date with E-Safety, child exploitation, grooming, FGM, LGBF, Sexting, Extremism and Gaming issues through guidance and liaison with the Local Authority E-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP) 4. The school's Computing subject leader and the Child Protection Co-ordinator ensures the Executive Headteacher, senior management and Governors are updated as necessary.

7.3 All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

7.4 All Staff (all teachers, supply staff and teaching partners) are reminded / updated about E-Safety matters at least once a year.

8. Handling E-Safety Complaints

8.1 The school will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

8.2 Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Staff and pupils are given information about infringements in use and possible sanctions.

8.3 It is the responsibility of parents to monitor the use of digital media outside of school . The schools will support parents to maintain e-Safety outside of school.

9. Sanctions available include:

- Discussion with E-Safety Coordinator / Executive Headteacher
- Informing parents or carers
- Removal of Internet or computer access for a period
- Referral to LA / Police

9.2 Subject leader acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Executive Headteacher. Any complaint about Executive Headteacher misuse will be referred to the Chair of Governors. Complaints of cyberbullying are dealt with in accordance with our Safeguarding Policy. Complaints related to child protection are dealt with in accordance with school / LA Child Protection procedures.

9.3 This policy is a working document and will be reviewed every two years. The Subject Leader will report to the Executive Headteacher, Head of School, Chair of Governors and staff on standards, achievements and make recommendations for future priorities.