BELMONT
PRIMARY SCHOOL
Inspire ~ Nurture ~ Flourish

1st November 2023
Next review date: 1st November 2025

E-Safety Policy

This policy comprises PART ONE of the School's E-Safety Handbook, available from the School Office.

CONTENTS

Throughout this policy 'parents' denotes those with parental responsibility.

1. Mission Statement

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. Belmont Primary School makes full use of these technologies to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. We believe access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use and that the School has a duty to provide pupils with quality Internet access. The School also recognises that pupils will use these technologies outside school and need to learn how to take care of their own safety and security. Belmont Primary School fully recognises its responsibilities for e-safety, including a responsibility to educate our pupils about the benefits and risks of using new technology and the provision of safeguards and information for all users to enable them to control their online experiences.

This Policy applies to all members of the school community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of school Information and Communication Technology (ICT) systems, both in and out of school. All adults, including volunteers, working in or on behalf of the School share the responsibility to keep children safe from harm

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this Policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

1.1 Aims and objectives

Our School aims to ensure that children are effectively safeguarded from potential risk of harm and that the safety and well-being of children is of the highest priority in all aspects of the School's work.

Specifically we aim to:

- ensure that all stakeholders are aware of and take seriously their responsibility to promote and safeguard the online safety of children;
- use the Internet and other technologies as tools for teaching and learning within the context of educating children and adults in how to use such technology responsibly, giving clear expectations for appropriate use;
- ensure staff and children understand the dangers that can arise and the procedures for dealing with e-safety incidents;
- ensure that school Internet access is appropriate for both pupil and adult use and includes filtering appropriate to the age of pupils;
- guide pupils in using technologies and developing skills in ways appropriate to their age and maturity.

2. Roles and Responsibilities

2.1 Governors

A member of the Governing Body has taken on the role of E-Safety Governor (Pat Devito, Deputy Child Protection Governor). Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy. Review of effectiveness will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. The role of the E-Safety Governor includes:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety Incident Logs
- regular monitoring of Filtering/Change Control Logs

- reporting to the governors' Community Committee

2.2 Head Teacher and Senior Leaders

The Head Teacher (or in her absence the Deputy or another member of the Senior Leadership Team) is responsible for:

- ensuring the E-Safety Policy is disseminated and its importance explained;
- ensuring the safety (including e-safety) of members of the School Community (although the day today responsibility for e-safety is delegated to the E-Safety Co-ordinator);
- ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable continuing professional development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as is relevant;
- ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- receiving regular monitoring reports from the E-Safety Co-ordinator;
- having familiarity with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Head Teacher is designated person for child protection and as such should be

- trained in e-safety issues;
- aware of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal/inappropriate materials; inappropriate online contact with adults/strangers; potential or actual incidents of grooming and cyber-bullying.

2.3 E-Safety Co-ordinator: Michelle Clifton

The E-Safety Co-ordinator has responsibility for:

- assisting the Head Teacher in making sure that the Policy is disseminated and clearly understood;
- taking day to day responsibility for e-safety issues and a leading role in establishing and reviewing the E-Safety Handbook;
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- providing training and advice for staff;
- liaising with the Local Authority;
- liaising with school ICT technical staff;
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments;
- meeting regularly with the E-Safety Governor to discuss current issues, review Incident Logs and Filtering/Change Control Logs;
- attending relevant meetings of the governors' Community Committee to give reports;
- reporting regularly to Senior Leadership Team;
- managing password security and allocating passwords for new users, and replacement passwords for existing users;
- carrying out an e-safety audit every two years and producing an action plan if necessary (refer to E- Safety Audit in E-Safety Handbook).

2.4 Network Manager

The Network Manager is responsible for ensuring that:

- the School's ICT infrastructure is secure and is not open to misuse or malicious attack with effective protection (e.g. firewall/anti-virus software) in place;
- the School meets the e-safety technical requirements outlined in any relevant Local Authority e-safety policy and guidance;
- users may only access the School's networks with allocated passwords, that are periodically changed;
- he/she keeps up to date with e-safety technical information in order to effectively carry out his/her e-safety role and to inform and update others as relevant;

- the use of the network, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator for investigation, action and/or sanction;
- the School's Filtering Policy (see section 10) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- the school filtering system is effectively managed and records/logs are kept of changes and of breaches of the filtering systems;
- there is a system of checks and balances to protect those responsible, changes must be reported to a second responsible person (E-Safety Co-ordinator) every term in the form of an audit of the Change Control Logs.

2.5 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the school Staff Acceptable Use Policy Agreement;
- they report any suspected misuse or problem to the E-Safety Co-ordinator;
- digital communications with pupils (email, voice, video) are only on a professional level and carried out using official school systems;
- e-safety issues are embedded in all aspects of the Curriculum and other school activities;
- pupils understand and follow the school E-Safety, Acceptable Use Policy and Google Classroom agreement;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they 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;
- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- they safeguard the security of their username and password and do not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security and MUST change their password immediately;
- they report immediately to the E-Safety Co-ordinator any infringements in the School's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered;
- they do not attempt to use any programmes or software that might allow them to bypass the filtering or security systems in place to prevent access to such materials.
- they at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- they use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
- they will 'lock' computers when they are not in use using the Windows key + L.

2.6 Pupils

Pupils are expected to:

- use the school ICT systems in accordance with the Pupil Acceptable Use Policy and Google Classroom agreement which they will be required to agree to before being given access to school systems;
- report abuse, misuse or access to inappropriate materials, once they know how to do so;
- know and understand school policies and procedures on the use of mobile phones, digital cameras and hand held devices including the taking or use of images;
- understand that cyber-bullying is a form of bullying and will not be tolerated;
- safeguard the security of their username and password and not allow other users to access the systems using their log on details. They should report any suspicion or evidence that there has been a breach of security so their password can be changed;

- understand the importance of adopting good e-safety practice when using digital technologies out of school and recognise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the School.

2.7 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through e-safety evenings, newsletters, letters, website and information about national and local e-safety campaigns or literature.

Parents will be responsible for:

- endorsing the Pupil Acceptable Use Policy and Google Classroom agreement;
- accessing the school website in accordance with the relevant School Acceptable Use Policy.

3. E-Safety Education

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children need the help and support of the School to recognise and avoid e-safety risks and build their resilience. E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

E-Safety education is provided in the following ways:

- a planned e-safety programme is provided as part of Computing /PSHE and should be regularly revisited – this will cover the use of ICT and new technologies both in school and outside school (e-safety is taught using the CEOP 'Thinkuknow' resources);
- pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school;
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- rules for use of ICT systems and Internet are posted in all rooms;
- staff act as good role models in their use of ICT, the Internet and mobile devices;
- Parents have access to Parent Zone (an online e-safety resource the school has subscribed to).

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

(Also see Internet Access, World Wide Web, Use of Digital and Video Images, Use of email, Use of Social Networking).

4. Internet Access

- All staff must read and agree to Acceptable Use Policy Agreement before using any School ICT resource.
- All pupils and parents will be asked to read and agree to an AUP form on entry to the school
- Parents will be informed that pupils will be provided with supervised Internet access.
- School Policy restricts certain Internet usage (refer to the Restricted Internet Usage table in E-Safety Handbook page 13)

5. World Wide Web

- Belmont Primary School use a London Grid for Learning (LGfL) filtered Internet Service, which will minimise the chances of pupils encountering undesirable material. The School will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff are aware of the potential for misuse and are responsible for explaining to pupils, the expectation we have of them. Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.
- Pupils will be guided to sites in lessons that have been checked as suitable and processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Pupils will be monitored when using the Internet when they are allowed to freely search, e.g. using search engines. Staff should be vigilant in monitoring the content of the websites the young people visit and they are expected to use age-appropriate search tools.
- The school never allows 'raw' image search with pupils e.g. Google image search.
- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Click On IT helpdesk via the E-Safety Co-ordinator or network manager.
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- There will be a 'no blame' environment that encourages pupils to tell a teacher or other responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

As part of the Computing curriculum, pupils are taught:

- to be critically aware of the materials and content they access on-line and to validate the accuracy of information;
- to know how to narrow down or refine a search;
- to be aware that the author of a website or page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- to understand the issues around aspects of the commercial use of the Internet, as age-appropriate. This may include, risks in pop-ups; buying online; online gaming or gambling;
- what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher.

6. Acceptable Use Policy and G Suite for Education Agreement

These Policies take the form of clear rules to which children, parents and staff indicate their agreement.
The AUP Policy reflects the use and responsibility of each group and their ability to take responsibility for their own use of the technology. There are therefore separate agreements for:

- Children
- Members of staff

Parents and children in are also required to agree to a G Suite for Education Agreement.

(Refer to AUP and G Suite for Education Agreement in E-Safety Handbook)

7. *Use of Digital and Video Images*

- When using digital images, staff are expected to inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Members of staff are allowed to take digital or video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. **Such images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Photographs published on the Website and Twitter, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on the School Website, in association with photographs.
- Permission from parents will be obtained before photographs of pupils are published on the School Website
- A designated member of School staff will maintain the School's Twitter account, as agreed by the Chair of Governors. They will follow the following protocol: tweets will only happen during school hours and the images will be deleted from their device.

As part of the Computing curriculum, pupils are taught:

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
- to understand why they must not post pictures or videos of others without their permission;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention.

8. *Use of Email*

- From Key Stage 2 (Year 4) onwards pupils may use LGfL 'Safemail' on the School system.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain letters is not permitted.
- Pupils are introduced to, and use email as part of the Computing scheme of work.

As part of the Computing curriculum, pupils are taught:

- not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent;
- that an email is a form of publishing, where the message should be clear, short and concise;
- that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- that they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
- to STOP and THINK before they CLICK and not open attachments unless sure the source is safe;
- that they must immediately tell a teacher or other responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening emails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them.

9. Use of Social Networking

The School blocks access to social networking sites and newsgroups unless a specific use is approved.

As part of the Computing curriculum, pupils are taught:

- never to give out personal details of any kind which may identify them or their location;
- not to place personal photos on any social network space;
- to set passwords, deny access to unknown individuals and block unwanted communications;
- to invite known friends only and deny access to others;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.

10. Filtering Policy

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can guarantee 100% protection against access to unsuitable sites. It is therefore important that the School has a policy regarding filtering to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Belmont is part of the Hounslow LGfL network and, in common with other connected organisations in the Local Authority, automatically receives the benefits of a managed filtering service, with some flexibility for changes at local level.

10.1 Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the E-Safety Co-ordinator who will decide whether to make school level changes. If it is felt that the site should be filtered (or unfiltered) at LGfL level, the Network Manager should click on the Send Comment button on the web page brought up when the site is blocked.

10.2 Monitoring

As the filtering system cannot guarantee 100% protection, the School monitors the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Policy. Monitoring will take place as follows:

10.3 Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the Head Teacher
- E-Safety Governor and/or Community Committee

The Filtering Policy will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring and/or disciplinary action might be necessary).

11. Password Security

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access;
- no user is able to access another's files, without permission (or as allowed for monitoring purposes within the School's policies);
- access to personal data is securely controlled in line with the School's policy (see section 12 below);
- logs are maintained of access by users and of their actions while users of the system ;

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email.

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access or data loss. This should apply to even the youngest of users, even if class logons are being used.

12. Data Protection/ GDPR

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Please refer to the Data Protection and GDPR Policy for further detail.

Sensitive data will be transferred using encryption and secure password protected devices only. (The Local Authority has a secure system for transfer of pupil data to and from schools and other services e.g. admissions, Social Care). Any data must be securely deleted from devices and secure sites, in line with school policy once it has been transferred. The School will monitor its use of portable computer systems, USB sticks or any other removable media, to ensure that any sensitive data cannot be linked to an individual unless the data is encrypted and password protected.
(Please refer to the School's Data Protection & GDPR Policy).

13. Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this Policy. However, there may be times when infringements of the Policy could take place, through careless or irresponsible use or, very rarely, through deliberate misuse.
For the handling of e-safety infringements the flow chart should be consulted and actions followed in line with it (refer to Flowchart for Responding to E-Safety Incidents in E-Safety Handbook), the Handbook lists the responses that will be made to any apparent or actual incidents of misuse:

If a pupil infringes the E-Safety Policy the incident will initially be referred their Team Leader. After repeated misuse, access to computers and/or the Internet in school may be removed for a specific time. Refer to Dealing with Pupil Incidents table (E-Safety Handbook) for how different incidents will be handled.

If a staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher. Refer to Dealing with Staff Incidents table (E-Safety Handbook) for how different incidents will be handled.

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The incident must be immediately reported to the Head Teacher, who will seek advice from the Local Authority and report to the police and Social Services as advised. Evidence should be preserved to assist investigation.

14. Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (See Safeguarding and Child Protection Policy)
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

15. Monitoring and Review of the Policy

- This Policy will be reviewed annually as part of the school's E-Safety Audit and referred to the governors' Community Committee should changes be necessary.
- The Head Teacher will report annually on e-safety and the implementation of this Policy to the Governing Body.