Belmont Infants School
Online Safety Policy
Inc. Social Media Use

The educational and social benefits for children in using the internet should be promoted, but this should be balanced against the need to safeguard children against the inherent risks from internet technology. Further, schools need to be able to teach children how to keep themselves safe whilst on-line.

This document provides guidance on developing an effective online safety strategy so that these aims can be achieved and support staff to recognise the risks and take action to help children use the internet safely and responsibly.

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

Schools must have a strategy in place for communicating the online safety policy to staff, pupils and parents and the policy document will be posted on the school's website.

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.

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

1. **The technologies**

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:
- Web browsing on the internet
- Instant messaging e.g. What'sApp, SnapChat
- Social networking sites e.g. Facebook, Instagram
- Video broadcasting sites e.g. YouTube, TikTok
- Gaming sites e.g. Roblox
- Chat rooms on sites such as Roblox
- Music download sites e.g. Spotify
- Smart phones with web functionality and apps
- E-mail
- Blogs
- Podcasts

2. **Whole school approach to the safe use of computing**

Creating a safe computing learning environment includes three main elements at Belmont Infant School:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive online safety education programme for pupils through Purple Mash and our HRE scheme SCARF.

3. Managing Internet Access and Information system security

Belmont Infant School:

- Maintains broadband connectivity through the London Grid for Learning (LGfL) and connects to the National Education Network;
- Ensures a safe online log in through LGfL to ensure children can access a variety of learning platforms safely and easily without searching through search engines;
- Works in partnership with the Local Authority (LA) to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect pupils;
- Ensures network health through appropriate anti-virus software and network set-up so staff and pupils cannot download executable files;
- Ensures their network is healthy by having health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the systems administrator/network manager is up to date with LGfL/Google Classroom services and policies;
- Has a system administrator/network manager that checks to ensure that the filtering methods are effective in immediately preventing access to any website considered inappropriate by staff;
- Never allows pupils access to internet logs;
- Never sends personal data over the internet unless it is secured;
- Ensures pupils only publish within appropriately secure learning environments such as Purple Mash;
- Pupil logs in, if not used, log out automatically after 20 minutes and after 3.30pm to avoid misuse.
- Teachers have online user names and passwords for all school subscriptions

4. Email

- Pupils may only use virtual e-mail accounts (Purple Mash) linked to curriculum based activities;
- Pupils must immediately tell a teacher if they receive offensive e-mail or anything they find upsetting or feel is wrong. This is taught within the online safety curriculum for all years;
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. This is taught within the online safety curriculum for all years;
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper;
- Teachers use email for professional communication; they update their password every sixweeks to ensure maximum security.

5. Images

- Staff / children do not include the full names of pupils in any published school video materials;
- Digital images of pupils are stored in the teachers' folders and images are deleted at the end of three years – unless an item is specifically kept for a key school publication;
- Staff / children do not use pupils' full names in file names when saving images;
- Staff teach pupils to save their images in their folders with a name relevant to the topic so the file can be easily identified;
- Parents will be asked to sign the online safety agreement form to indicate their agreement to their children's images being used on school's website or for other purposes.

6. Using the School Network and System

Belmont Infant School:

- Makes it clear that staff must keep their log-in username and password private and must not leave them where others can find them. We do not share these with any supply staff;
- Requires all users to log off when they have finished working or lock the computer when leaving the computer unattended;

- Where a user finds a logged-on machine, we require them always to log-off and then log-on again as themselves;
- Children log on using the class username and password. Work can be saved in their independent drive.

7. Managing video conferencing

Belmont Infant School:

- Uses Zoom and Teams for staff training and some meetings;
- Uses Zoom for remote learning and expects all children to access via their parents account;
- Expects staff, children and parents to be appropriately dressed when accessing video learning via Zoom.

8. Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in Belmont Infant School and the Head, 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 compliance with the policy monitored. The responsibility for Online safety has been delegated to the Computing Lead, Shauna Sweeney.

Our computing lead ensures Belmont Infants keeps up to date with online safety issues and guidance through liaison with the network administrator, LA Computing advisers, Computing leads' meetings (NLC) and organisations such as Britain's Educational Communication and Technology Agency (Becta) and The Child Exploitation and Online Protection (CEOP) Centre.

The school's computing lead ensures the Headteacher, SLT and Governors are updated as necessary and ensures that Belmont Infants covers the statutory curriculum for computing and online safety. They monitor and evaluate the curriculum throughout the year ensuring that children gain experience in all aspects of computing, in line with the policy.

Governors need to have an overview and understanding of online safety issues and strategies at Belmont Infant School. Belmont Infants ensures the governors are aware of the local and national guidance on online safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online safety procedures. Central to this is fostering a 'No blame' culture so pupils feel able to report any bullying, abuse or inappropriate material.

Teachers should ensure that pupils are aware of the online safety rules, introducing them at the beginning of each new school year and at other points throughout the year.

Teachers should ensure that pupils are aware of the online safety rules, introducing them at the beginning of each new school year and at other points throughout the year.

All staff should be familiar with the schools' policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networks;
- Safe use of school network, school social media, equipment and data;
- Safe use of digital images and digital technologies, such as cameras and iPads;
- Publication of pupil information/photographs: use of website and social media;
- Procedures for dealing with on-line bullying;
- Their role in providing online safety education for pupils as per the curriculum;
- Discussion of online safety issues at least once a year when this policy is reviewed;
- Staff must not communicate with students using public social networking sites such as WhatsApp, Facebook, Twitter, etc.

Belmont Infant School:
- Supervises pupils' use of ICT as far as is reasonable, and is vigilant in learning resource areas
- Informs users that internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to Shauna Sweeney. Our system administrator reports system failures that may put pupils at risk to the LA as necessary;
- Blocks all chat rooms and social networking sites except those that are of an educational network or approved learning platform;
- Only uses approved or checked webcam sites;
- Uses closed, online subscriptions for curriculum based learning;
- Ensures all users know and understand the rules of appropriate use and what sanctions result from misuse through staff meetings and teaching programmes;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures parents provide consent for pupils to use the internet, as well as other computing technologies, as part of the online safety acceptable use agreement which parents are asked to sign at the time their child enters the school;
- Immediately refers any material we suspect is illegal to the appropriate authorities: LA or Police.

9. Internet Use
Belmont Infant School:
- Encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;

- Ensures that staff preview any recommended sites before use;

- Does not allow pupils to make raw image searches using Google images;

- Ensures that when Internet research is set for homework, sites are suggested that have previously been checked by the teacher;

- Ensures pupils and staff know what to do if they find inappropriate web material i.e. switch off monitor and report the URL to the teacher/ online safety lead;

- Ensures pupils and staff know what to do if there is an online or cyberbullying incident;

- Teaches pupils 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;

- Ensures that, as far as practicable, the use of Internet derived materials by staff and pupils complies with copyright law;

- Delivers an online safety programme of support to parents who have an important role in supporting safe and effective use of the internet by pupils;

- Ensures that all our pupils have access to the Internet, particularly where this will directly support their learning;

- Ensures that there is no unsupervised access to the Internet at any time.

10. Social Media
Social media and social networking sites play an important role in the lives of many people. We recognise that using social media bring risks, but equally there are many benefits to be gained. This policy provides clarity to the way in which social media are to be used by pupils, governors, visitors, parent helpers and school staff at Belmont Infant School. It will also provide guidance for parents.

11. Use of social media by staff in a personal capacity
Social media covers a range of internet based technologies that have been developed to enhance and improve the way we communicate and interact with others. A social media networking service is an online service, platform, or site that focuses on facilitating the building of social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections.

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts

in an appropriate manner.

Guidelines are issued to staff:
- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16) – it must be reported to the Headteacher or designated CP lead;
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts;
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the governing body;
- Staff must not use social networking sites on the school site (for personal use).
- Staff should only use social networking in a way that does not conflict with the current national teacher's standards;
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality;
- Staff should not share any personal information with any pupil; including personal contact details, personal website addresses or social networking site details.
- If staff are online 'friends' with any parent/carer linked with the school, they must ensure that they do not disclose any information or otherwise post details which may bring themselves or the school into disrepute. Staff must not engage in any online discussion about any child attending the school.
- School staff must not disclose, on any social networking site, any information that is confidential to the school, Governing Body, or Local Authority; or post anything that could potentially bring the school, Governing Body or Local Authority into disrepute.

12. Use of social media by staff in a professional capacity
- Staff must not disclose any personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act.
- Staff should not post photographs of pupils under any circumstances, and should not post photographs of colleagues or others in the school community, without their express permission, onto personal social media sites.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.
- Care should be taken to avoid using language which could be deemed as offensive to others.

13. Use of social media by parents/carers
Parents and carers will be made aware of their responsibilities regarding their use of social media. Methods of school communication include: the prospectus, the website, newsletters, letters, texts and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving issues. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents have a responsibility to ensure that their use of social media exemplifies best practice and need to understand that they are role models for their children. Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event. If parents wish to complain about anything pertaining to school, they should make complaints through official school channels rather than posting them on social networking sites. Parents should not post malicious or fictitious comments on social networking sites about any member of the school community whether it be another parent, child or staff member.

14. Breaches of the Policy
- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion;
- While the Governing Body does not discourage school staff from using social networking sites, staff should be aware that the Headteacher/Governing Body will take seriously any circumstances where such sites are used inappropriately, including any usage that is considered to be online bullying or harassment;
- The Headteacher may exercise his/her right to monitor the use of the School's information systems,

including internet access, where it is believed unauthorised use may be taking place. If such monitoring detects the unauthorised use of social networking sites, disciplinary action may be taken;

- If any instances or allegations of inappropriate use of social networking sites are brought to the attention of the Headteacher/Governing Body, disciplinary action may be taken;
- The Governing Body reserves the right to take action to remove any content posted by school staff which may adversely affect the reputation of the school or the wider school community, or put it at risk of legal action.

15. How will complaints regarding online safety be handled?

The School will take all reasonable precautions to ensure online 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. Neither the School nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are informed of the possible consequences of any infringements in the use of Computing:
- Referral to Headteacher
- Informing parents/carers
- Possible removal of internet or computer access for a fixed period
- Referral to LA/Police.

The Headteacher is the first point of contact for any complaint; including staff misuse. Complaints of on-line or cyber bullying are dealt with in accordance with our Behaviour Policy which includes our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school/LA child protection procedures

Parent Guidance – Useful Websites

ThinkUKnow - useful section for parents and carers

Bullying UK - section on cyber-bullying

KidScape - an organisation with advice on preventing bullying and child abuse

Vodafone Digital Parenting - information for parents about e-safety issues

Parenting, Media, and Everything In Between | Common Sense Media - explanations about ratings and content on all games and films

Advice on Parental Control Tools:

Childnet International - includes practical guides for setting up controls

ThinkUKnow - advice about internet service providers and parental control

What Are the Best Privacy Settings for My Kid's Apps and Devices? | Common Sense Media – everything you need to know about controls for all platforms and games