BELMONT SCHOOL

(Additionally Resourced Mainstream School)

E-Safety/Online Safey and Acceptable Use of Computing Systems Policy 2023

UNCRC Article 19 -
Every child has the right to protection.
Global Goal 3 - Good Health and Well-being
Ensure healthy lives and promote well-being for all at all ages.
Global Goal 10 - Reduced Inequalities
Reduce inequality within and among countries.

Head Teacher	
Name	Mrs P Aggarwall
Chair of Governors	
Name	Mr M Kara
Date Ratified	10th October 2023
Review Date	September 2024

This policy is linked to the following mandatory school policies: Keeping Children Safe in Education – September 2023 guidance, Safeguarding and Child Protection, Preventing Radicalisation and Extremism, SEND, Code of Conduct, Whistle Blowing, Health and Safety, Behaviour, Anti-Bullying policies and Home School agreement.

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Safeguarding and Promoting the Welfare of Children at Belmont School Key Contacts:

Role	Name	Telephone	email
Designated Lead Person for Safeguarding (DSL)	**Mrs L. McKenzie.**	**02084270903**	**office@belmont.harrow.sch.uk** **cp@belmont.harrow.sch.uk**
Deputy DSL	**Mrs P. Aggarwall**	**02084270903**	**office@belmont.harrow.sch.uk** **cp@belmont.harrow.sch.uk**
Designated Lead Governor for Safeguarding	**Mr M. Kara**	**02084270903**	**office@belmont.harrow.sch.uk**
Lead for Looked After Children	**Mrs P. Aggarwall**	**02084270903**	**office@belmont.harrow.sch.uk** **cp@belmont.harrow.sch.uk**
Lead for On-line Safety	**Mrs P. Aggarwall**	**02084270903**	**office@belmont.harrow.sch.uk** **cp@belmont.harrow.sch.uk**
Headteacher (for concerns/allegations about staff	**Mrs P. Aggarwall**	**02084270903**	**office@belmont.harrow.sch.uk** **cp@belmont.harrow.sch.uk**

(i) Key local contacts for safeguarding children

Harrow Children's Social Care & Multi-agency Safeguarding Hub (MASH)	**'Golden Number': 020 8901 2690** **Emergency Duty Team** :weekends, bank holidays and between 5pm-9am during the week: **020 8424 0999**
Police	**101 or for immediate emergency: 999**
FGM - Mandatory reporting	Police on 101
Local Authority Designated Officer for Allegations against staff (LADO)	Initial referrals via MASH/Golden Number above. **Ongoing cases: 020 8736 6435**
Children and Young People with Disabilities 0-25 years	**020 8966 6481**
Local multi-agency procedures, guidance and Training: Harrow Safeguarding Children Board	**www.harrowlscb.co.uk**
NSPCC	**0800 800 5000**
Childline	**0800 1111**
Government's Whistle-blowing Service via NSPCC Report Line	**0800 028 0285**

Belmont School's Vision

Development of the whole school learning community promotes personalised and independent learning throughout the learning journey for pupils and adults. Pupil voice informs all school development priorities – every child, every day make us 'Stronger Together'.

Introduction

Keeping Children Safe in Education, September 2023, states that:

> ***"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate".***

This policy seeks to raise awareness for pupil's stay safe, and that they be protected from harm and neglect and grow up able to look after themselves.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Belmont School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Belmont School
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

What is online safety?

Online safety is defined as educating people about the benefits, risks and responsibilities of using the internet and electronic devices. Online safety is:

- Safeguarding children in the digital world
- Not about restricting children, but educating them
- Supporting children and young people to develop safer online behaviours both in and out of school.
- Being educated ourselves to be able to support and help the children.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk as outlined in Keeping Children Safe in Education, September 2018:

Content:

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact:

- Grooming
- Cyber-bullying in all forms
- Identity theft and sharing passwords

Conduct:

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Online Radicalisation (Radicalisation is the process by which an individual or group comes to adopt increasingly extreme political, social, or religious ideals and aspirations. The internet offers opportunities from online radicalisation to spread easily)

This policy applies to all members of Belmont School (including staff, supply staff, pupils, governors, parents / carers, volunteers and visitors) who have access to and are users of school computer systems both in and outside of Belmont School.
The school is aware that all members of the school community are at risk of breaching online safety protocols.

The Education and Inspections Act 2006 empowers Headteachers 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 online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for, and of, electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

All staff have a duty of care to the pupils that are in our school. We are all responsible for all aspects of pupil safety, including online safety, whilst in school. We must teach the children online safety skills regularly to help them develop safe online behaviours. Any activity involving internet use needs to be carefully planned and assessed for risk to minimise the possibility of an online safety incident.
If an online safety incident occurs outside of school and affects our children, the school must deal with the incident.

The following section outlines the online safety roles and responsibilities of individuals within our school.

Governors:

The Governors are responsible for:

- The approval of the E Safety and Acceptable Use of ICT Systems policy and for reviewing its effectiveness. This will be carried out by the Governors receiving termly information about any reported online safety incidents.
- Providing a member of the Governing Body to take on the role of monitoring online safety linked in with monitoring safeguarding.
- Reading, understanding, and signing the Governor Acceptable Use Policy (AUP).

Head teacher:

The Headteacher has a duty of care for ensuring the safety (including online safety) of all members of the school community, though the day-to-day responsibility for online safety is delegated to the Computing Co-ordinator.

The Head teacher is responsible for ensuring:

- That they, SLT and the Computing Co-ordinator are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Computing Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

Designated Safeguarding Lead:

The Designated Safeguarding Lead should be trained in the online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/ inappropriate materials.
- Inappropriate online contact.
- Potential or actual incidents of grooming.
- Cyberbullying.

Computing Lead:

The Computing Lead has the day-to-day responsibility for online safety. They are responsible for:

- Leading the day-to-day responsibility for online safety issues and has a leading role in reviewing the school E-Safety and Acceptable Use Policy and documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for all members of the school community.
- Ensuring all pupils understand and follow the online safety and acceptable use policy.
- Ensuring online safety is embedded into the curriculum.

Technical Staff (IT Technician, School Business Manager):

The IT Technician and Technical Support (Beebug) are responsible for ensuring:

- That the school's technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets the required online safety technical requirements that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- That the use of the network, internet, website, remote access, and email is regularly monitored in order that any misuse or attempted misuse can be reported to the ICT Co-Ordinator and the Headteacher.
- Liaising with technical staff (Beebug).
- Reporting regularly to the Headteacher with regards to online safety.

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and the E-Safety and Acceptable Use of ICT Systems policy and practices.
- They have read, understood, and signed the Staff Acceptable Use policy (AUP). Staff should be aware that internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.
- They report any suspected misuse or problems to the Computing Co-ordinator and Headteacher for investigation, action, or sanction.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
- Online safety is embedded into their teaching and that sites are checked for suitability before using them with the pupils.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Pupils:

The pupils are responsible for:

- Using the school system in accordance with the pupil acceptable use policy (AUP).
- Reporting an abuse, cyberbullying, misuse, or access to inappropriate materials.
- Understanding the importance of being safe online.
- Adopting good online safety practice when using digital technologies outside of school and understanding that the school E-Safety and Acceptable Use of ICT Systems policy covers their actions out of school, if related to school.

Parents/ Carers:

A partnership approach with parents/carers will be encouraged as parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand the issues relating to online safety through parent workshops, school newsletters and the website and internet issues will be handled sensitively to inform parents without undue alarm. Parents and Carers are encouraged to support the school in promoting good online safety practice and follow the guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parent sections of the website
- Social Networking Sites
- Mobile Phones
- Their children's personal devices which access the internet

Why is the use of ICT systems so important to our pupils and staff?

- The purpose of ICT and internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- ICT and internet use are a part of the statutory curriculum and a necessary tool for staff and pupils.
- ICT and internet access are an entitlement for pupils who show a responsible and mature approach to its use.
- ICT and the internet are essential elements in life for education. The school has a duty to provide pupils with quality ICT systems and Internet access as part of their learning experience.

Why internet use is important.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils and will enhance learning.

- The school internet access will be designed expressly 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 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.
- ICT use and internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- As much as possible, the school's chosen internet service provider has organised information resources in ways that point pupils to those that have been reviewed and evaluated prior to use.

How will pupils learn to evaluate internet content?

- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its validity.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Advice will be available to staff in the evaluation of web materials and methods of developing pupils critical attitudes.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Head teacher and Computing Co-ordinator/s.

Computer System Use

- Adult users need to sign the Acceptable Use Policy.
- Parents/carers of children are required to sign an Acceptable Use Policy on behalf of their child.
- The school will keep a record of all staff and pupils who are granted ICT and internet access. The record will be kept up-to-date, e.g. staff may leave or a pupil's access be withdrawn.
- For EYFS and Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Children without internet access may have access to the computers at breaks and lunch times which is monitored by staff.
- Appropriate training for pupils will be delivered – aspects of E-Safety will be included in most ICT Lessons.

Computer System Security

- The Headteacher has overall responsibility for the security of the computer systems.
- The school ICT systems capacity and security are reviewed regularly.
- Virus protection and anti-spyware is installed and updated regularly.
- Security strategies will be discussed with the Local Authority, particularly where a wide area network connection is being planned.
- School approved email system will be scanned for virus.
- Personal data sent over the internet is encrypted or otherwise secured.

- Use of portable storage media such as USB memory sticks, DVDs, CD-ROMs and other storage devices will be reviewed. Where applicable such devices will comply with latest guidance on Handling Sensitive Data. At the very least, all USB and portable drives used to store sensitive data are encrypted and password protected.
- Portable media may not be brought into school by pupils without specific permission and a virus and spyware check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to emails.
- Staff and pupils will be made aware that files and communications on the school ICT equipment are not private and may be reviewed.
- The school will arrange for a selective search of the network server's hard drive to be carried out on a regular basis to monitor images in users' folders.
- The school will arrange for the hard drives in staff laptops and other PCs to be reviewed on a regular basis to monitor images.

Password Security

- All users are provided with a username and password generated by LGFL Atomwide.
- The Technical Team keeps an up-to-date record of users and their usernames. The "administrator" passwords for the school computer system, used by Beebug, must also be available to the Headteacher and Computing Co-ordinator and kept in a secure place. The record is kept up to date, e.g., staff may leave, or a pupil's access may be withdrawn. Any new systems administer must remove staff as and when they leave.
- All users with access to the computer systems are responsible for taking the appropriate steps to select and secure their passwords.

These steps should include:

- Keeping their password secure from other people.
- Staff and children should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- Passwords shall not be revealed to unauthorised persons.
- Passwords shall not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g., when a password may be known by an unauthorised person.
- When leaving a computer for any length of time, everyone shall log off or lock the computer, using CTRL+ATL+DELETE.
- All users must immediately report any suspicion or evidence that there has been a breach of security.

Managing filtering

- The school will work with Bee Bug, LGFL, LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school's broadband access includes filtering appropriate to the age and maturity of pupils. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.
- Emerging technologies will be examined for educational benefit and the Head teacher in consultation with staff will give permission for appropriate use.

- Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head teacher, so that pupil mobile phones can be kept in the school office. Parents must write a consent letter to acknowledge that the school takes no responsibility for phones which are left in a secure location.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Staff should not use their personal mobile phone to contact pupils or pupil's families and therefore this will only be done when authorised by a senior member of staff or in the case of an emergency.
- Abusive messages should be dealt with under the school's behaviour and safeguarding policy.
- Access to images will be restricted by using the 'safe search' option within the search engine, although this is not completely safe. It is recognised that when pupils or staff use a search engine for images, they may find inappropriate material. Staff and pupils will be encouraged to use child friendly sites where possible.
- If staff or pupils discover unsuitable sites or material that is illegal, the URL must be reported to a senior member of staff and the Computing co-ordinator. These URL's will be recorded on the online and the appropriate agencies informed.

Transportation of Sensitive Material – Use of External Hard Drives and 'Cloud based' services.

- All staff will be made aware of the issues surrounding confidentiality and safeguarding regarding the transportation of information outside of the school gates.
- All staff who are required to transport sensitive information regarding pupils are to be trained as to how to safely transport this data.
- All staff are expected to take the proper precautions when removing information such as electronic planning and resources from the school server to their home PCs – this information in no way will name or describe members of the class or members of the school role.

Asset disposal

- Details of all school-owned hardware are recorded in a hardware inventory.
- Details of all school-owned software are recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency (Beebug).

This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

School's Information Systems (Arbor) and Website Security

- The data protection procedures provide information about physical, and systems security of data held on the school's information systems.
- Staff are issued with individual usernames and passwords to access Arbor. Their access rights are related to their role.
- We have created a website to celebrate pupils work, promote the school and publish resources for projects. Procedures and practice ensure website safety.

- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate however the Head teacher can delegate to the relevant person(s) editorial responsibility to ensure that the website content is accurate, and quality of presentation is maintained. The website is also checked regularly by a member of the Governing Body.
- The point of contact on the website is the school address, school email and telephone number. Staff or pupils' personal information will not be published.
- Most material is the school's own work; where others work is published or linked to, we credit the sources and state clearly the author's identity or status.
- Publication of information should be considered from a personal and school security viewpoint.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
- Written permission from parents or carers is obtained before photographs/videos of pupils are published on the school web site. If a parent changes their mind, they must inform the Headteacher in writing.
- Website photographs/videos that include pupils are selected carefully and pupils' names are not used anywhere on the website when in association with photographs/videos. We do not include the full names of pupils in the credits of any published school produced video materials/DVDs.
- We will ensure that before any images are uploaded to our website or published electronically, they are renamed so that the name of the pupil cannot be read by right clicking on the image.
- The copyright of all material will be held by the school or be attributed to the owner where permission to reproduce has been obtained.
- The web site should comply with the DFE guidelines.

<u>Use and storage of digital and video images.</u>

- Digital images /videos 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.
- Staff will not use their own personal devices including mobile phones, cameras, and tablets to take images of pupils.
- 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 online safety education programme.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

<u>Communication</u>

A wide range of communication technologies are available and used within the school including email, School Ping text system, parent pay and website. When using communicating technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users are aware that their email communications are monitored. Therefore, staff and pupils should only use the school email system to communicate with others.
- Users must immediately report any communication that makes them feel uncomfortable. If offensive, threatening or bullying in nature the user must not respond to any such communication.
- Any digital communication between staff and parents/pupils and the wider community must be made through official school communication systems and must be professional in tone and content.
- All communications are to be courteous and respectful of professional's experience and status and be compliant with GDPR. Forwarding email chains is to be avoided unless necessary. The best practice is to send a new email to the relevant colleague.
- 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.
- The forwarding of chain letters is not permitted.
- Pupils are taught about the online safety issues relating to communication and strategies to support the pupils if they encounter inappropriate communications.
- Pupils may not use personal email in the school.
- Access in school to external personal email may be blocked.
- Staff will not attach unencrypted sensitive data to emails. If sensitive data must be sent via the internet it will be sent securely.

Mobile Phones/ Handheld Mobile Devices

Personal Mobiles – Staff:

We recognise that mobile phones provide a useful means of communication. However, staff should follow the rules with regards to using mobile phones at work:

- Staff are not permitted to make/receive calls/texts during contact time with children.
- Staff should have their phones on silent or switched off and out of sight (e.g., in a drawer or handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g., classroom, playground).
- Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g., in office areas, staff room, empty classrooms.
- It is also advised that staff security protect access to functions of their phone.
- Should there be exceptional circumstances (e.g., acutely sick relative), then staff should make the Head teacher/SLT aware of this so that they can have their phone in case of having to receive an emergency call.
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras.
- Staff should report any usage of mobile devices that causes them concern to the Head teacher.

Mobile Phones for work related purposes:

We recognise that mobile phones provide a useful means of communication on off- site activities. However, staff should ensure that:

- Mobile use on these occasions is appropriate and professional (and will never include taking photographs of children).
- Mobile phones should not be used to contact parents during school trips unless it is an emergency and the Headteacher or a member of SLT has authorised this. Generally, all relevant communications should be made via the school office.
- Where parents are accompanying trips, they are informed not to contact other parents (via calls, text, email, or social networking) during the trip or use their phone to take photographs of children.

Personal Mobiles – Pupils:

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Many children have unlimited and unrestricted access to the internet via 3G and 4G on their phones, therefore.

- Pupils are not permitted to have mobile phones on their person at school or on trips.
- If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school if they are traveling home on their own, the following procedure must be followed:

The parent must provide written consent before a mobile phone can be brought into school . Once written consent has been obtained, the child can bring a mobile phone to school. The phone must be switched off and handed in to the class teacher first thing in the morning for it to be stored in the school office. The phone can then be collected at home time. The phone is left at the owner’s own risk.

- Mobile phones brought to school without permission will be confiscated and parents will be asked to collect the phone at the end of the day.
- Where mobile phones are used in or out of school to bully or intimidate others, then the Head teacher does have the power to intervene ‘to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site’.

Personal Mobiles- Volunteers, Visitors, Governors, and Contractors:

All volunteers, visitors, Governors, and contractors are expected to follow our mobile phone policy as it relates to staff whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones.

Personal Mobiles- Parents:

While we would prefer parents not to use their mobile phones while at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication.

We therefore ask that parents' usage of mobile phones, whilst on the school site is courteous and appropriate to the school environment.

We do not allow parents to photograph or video school events such as shows or sports day using their mobile phones.

Belmont School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. In such circumstances, the police may be contacted.

Social Networking and Personal Publishing

The school is aware that social networking is used widely for professional and personal purposes. However, parents and teachers need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

The school has a responsibility to provide guidance and training to ensure that all social networking use is safe and responsible. The school will block/filter access to social networking sites. News groups will be blocked unless a specific use is approved.

Social Networking - Staff:

- Staff are trained, as a part of their online safety training, about the risks of social networking.
- Staff are advised to not refer to matters of school business when engaging with or on social networking sites.
- Staff are advised to act professionally online.

All school staff should be aware when using social networking sites that anything said, shown or received could be made available to a wider audience than originally intended. They should follow and understand the following principles:

- Employees and individuals otherwise engaged by the school are not permitted to access social networking sites for personal use via school information systems or school equipment at any time.
- They must not accept pupils as 'friends' and must not approach pupils to become their friends on social networking sites. Personal communication of this nature could be considered inappropriate and unprofessional and make that individual vulnerable to allegations.

- Any pupil-initiated communication, or on-line friend requests must be declined and reported to the Headteacher or Designated Safeguarding Lead.
- Staff are advised not to be online friends with ex or recent pupils of the school or other schools.
- They should not share any personal information with any pupil, including personal contact details, personal website addresses or social networking site details.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger, and many others.
- Staff cannot under any circumstances mention any references to their working lives on any social media.
- 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 on-line 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.
- Staff must not disclose any personal data or information about any individual/colleague/pupil, which could be in breach of the GDPR.
- 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.
- Care should be taken to avoid using language which could be deemed as offensive to others.
- Staff are strongly advised to take steps to ensure their on-line personal data is not accessible to anybody they do not wish to access it. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum.

<u>Social Networking - Pupils:</u>

- Pupils do not have access to social networking sites on the school system.
- Pupils are advised of the age restrictions on social networking sites and the risks of social networking through their E-Safety lessons. Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests, and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals. Pupils should be encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, or defamatory.
- Pupils must immediately tell a teacher if they receive offensive email.

Social Networking - Parents:

- The school recognises that many parents and other family members will have personal social networking accounts which they might use to discuss/share views about school issues with friends and acquaintances. However, it is not the way to raise concerns or complaints as the school will not respond to issues raised on a social networking site. If there are serious allegations being made/concerns being raised, social media or internet sites should not be used to name individuals and make abusive comments.
- Parents 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.

The school considers the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):

- Naming children or posting any comments about children who attend Belmont School.
- Making allegations about staff or anyone else connected with the school.
- Making any posts that could be deemed to be cyber-bullying.
- Making complaints about the school or staff at the school
- Making defamatory statements about the school or staff at the school.
- Posting negative or offensive comments about staff or any other individual connected to the school.
- Posting racist comments.
- Posting comments which threaten violence.
- Posting comments or engaging in online discussions with children other than their own.

- **Procedure the school will follow if inappropriate use continues.**

- The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step the school will usually discuss the matter with the parent to try to resolve it and to ask that the relevant information is removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the school considers inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this.
- Set out the school's concerns to the parent in writing, giving a warning and requesting that the material in question is removed.
- Contact the police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is considered to be grossly obscene, grossly offensive or is threatening violence.
- Contact the host/provider of the social networking site to complain about the content of the site and ask for removal of the information.
- Take other legal action against the individual following appropriate advice.
- We are committed to resolving difficulties in a constructive manner, through an open and positive dialogue. However, we understand that everyday misunderstandings can cause frustrations and have a negative impact on our relationships. Where issues arise or misconceptions take place, please contact your child's teacher, who will be available to meet with you and go through the issue and hopefully resolve it. Where issues remain unresolved, please follow the school's complaints procedure. This is available on the school website, or a copy can be requested from the school office.
- Parents have opportunities to find out more about social networking sites by attending parent workshops.
- Parents are advised to follow the school social media rules at home with their children.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised, and the importance of chat room safety emphasised.

Managing emerging technologies and assessing risks

The digital age is ever changing, and new technologies are consistently emerging. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
Neither the school nor Harrow LA can accept liability for the material accessed, or any consequences resulting from internet use. Methods to identify, assess and minimise risks will be reviewed regularly and after every breach of this policy.

Training and Online Safety Education

Staff:

All staff receives online safety training and understands their responsibilities. Training is offered as follows:

- All new staff receives online safety training as part of their induction programme, ensuring that they fully understand the school E-Safety and Acceptable Use of ICT Systems policy.
- The Computing Co-Ordinator receives regular updates through attendance at training sessions and by reviewing guidance documents released by CEOP (Child Exploitation and Online Protection Command) / LGFL / LA and others.
- This policy and its updates will be presented to and discussed by staff in staff meetings and the staff/Governor's safeguarding newsletter.
- The Computing Co-Ordinator provides advice, guidance and training to individuals as required.

Governors:

Governors should take part in online safety training sessions, with particular importance for those who are involved in safeguarding and child protection. This is offered in several ways:

- Attendance at training provided by the Local Authority.
- Participation in school training / online training, information sessions for staff or parents and the staff/Governors safeguarding newsletter.

Pupils:

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. The school uses a range of resources to help with teaching online safety.

Online safety education is provided in the following ways:

- A planned online safety programme is provided as part of computing and other lessons and is regularly revisited – this covers both the use of computers and new technologies in school and outside school.
- Key online safety messages are reinforced during assemblies.
- The school promotes and celebrates Safer Internet Day.
- Pupils are taught in all lessons to be critically aware of the materials and content they access online and are guided to validate the accuracy of information.
- Pupils are encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside school.
- Staff should act as good role models in their use of ICT, the internet, and mobile devices.
- Pupils are informed that network and internet use is monitored and appropriately followed up.
- Pupil instruction in responsible and safe use should precede internet access every time they go online.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are vulnerable.

Below are examples of some of the E–Safety programmes that we may use:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Safe Social Networking: www.getsafeonline.org
- The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk
- Parent Zone and Google have developed "Be Internet Legends" - a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.

Children with Special Educational Needs and/or Disabilities:

Children with Special Educational Needs and/or Disabilities may be more vulnerable to risk from use of the internet and may need additional guidance on e-safety practice as well as closer supervision. Staff may wish to discuss this with parents and carers and help them to access information and resources from specialist agencies.

Parents/Carers:

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school therefore seeks to provide information and awareness to parents and carers through:

- Access to online safety policy.
- Parents training and workshops.
- School newsletter updates.
- Parent leaflets.
- Parent Acceptable Use.

Record keeping

- All serious incidents involving the use of technology will be logged centrally by the Senior Leadership Team and as part of the pupil or staff record.
- The records created in accordance with this policy may contain personal data. The school has a privacy notice which explains how the school will use personal data about pupils and parents. The privacy notice is published in the School Brochure on the School's website. In addition, staff must ensure that they follow the European General Data Protection Regulations (GDPR) when handling personal data.

How will the policy be introduced to pupils?

- Rules for ICT systems and Internet access will be posted around the school.
- Pupils' opinions will be consulted regarding the developments of the ICT Curriculum and how it may impact on their learning.
- Pupils will be informed that computer and internet use will be monitored.
- Instruction in responsible and safe use of the ICT systems and internet will precede access to them. E-safety is planned into the ICT Curriculum covering both home and school use.

How will staff be consulted?

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.
- All staff including teachers, Teaching Assistants, support staff and supp ly staff, will be provided with the E-Safety and Acceptable Use of ICT Systems policy, and its importance explained.
- Staff should be aware that computer and internet traffic could be monitored and traced to the individual user. Discretion and professional conduct are essential. The monitoring of internet use is a sensitive matter. Adults who operate monitoring procedures should be supervised by the Head teacher.

Breaches of the Policy - Reporting/Complaints/Sanctions

All staff and pupils have a responsibility to report online safety incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the pupils, staff or school.

- Responsibility for handling incidents is delegated to the Head teacher. Any complaint about staff misuse must be referred to the Head teacher. In the case of the Head teacher, any complaint must be referred to the Chair of Governors.
- 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 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.
- 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.
- Pupils and parents will be informed of the complaint's procedure via the Rules for responsible Internet and computer network use guidelines.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and Child Protection Procedures.
- The use of the CEOP button can be issued in serious online safety issues.

- The school has a responsibility to deal with cyber bullying reports whether it is happening inside school or outside school.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the Police must be contacted to establish the legal position and discuss strategies.

Sanctions for misuse include:

- Interview by Head teacher/SLT/ICT Co-ordinator
- Informing parents or carers
- Removal of Internet or computer access for a period which could ultimately prevent access to files held on the system
- When applicable, police or local authorities may be involved.
- Online safety incidents will be recorded on the online by the Computing Co-Ordinator or Head teacher. The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Head teacher.

Writing and reviewing the E-Safety policy

- The school has an ICT Co-ordinator who works closely with the Designated Safeguarding Lead as the roles overlap.
- The school will regularly self-audit due to technology changing rapidly.
- The E-Safety and Acceptable Use of ICT systems policy and its implementation will be reviewed annually by the Head teacher and Governors.

Abbreviations and Acronyms

ICT – Information and communications technology
AUP – Acceptable Use policy
SLT – Senior Leadership Team
CPD – Continuing Professional Development
LA – Local Authority
LGFL – London Grid for Learning
DFE – Department for Education
URL - Uniform Resource Locator (or web address)
EYFS – Early Years Foundation Stage
GDPR - General Data Protection Regulation
CEOP - Child Exploitation and Online Protection Centre

Appendix 1: Other E-safety Issues

Cyberbullying

Cyberbullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass, threaten or intimidate someone. Cyberbullying is often done by children, who have increasingly early access to these technologies.
It is essential that pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. This is done by:

- Promoting a culture of confident users will support innovation and safety.
- The NSPCC and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying:
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of bullying:
- Pupils, staff, and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying, and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include:
- The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time. Parent/carers will be informed, and the Police will be contacted if a criminal offence is suspected.

Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.

Pornography – many children will come across some type of pornographic content when searching the internet. Children are taught about what to do if they come across this type of material and who to speak to.

Contact with violent extremists - Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences. Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.

Belmont School will ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.

Acceptable Use Policy (AUP) for PARENTS

What is an AUP?

We ask all children, young people and adults involved in the life of Belmont School to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP (a copy is available on the school website)

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong, and people can get upset, but these rules should help us avoid it when possible and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read Belmont Schools full Online Safety Policy (see the school website) for more detail on our approach to online safety and links to other relevant policies (e.g., Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to your child's class teacher.

What am I agreeing to?

1. I understand that Belmont School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks, and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible, and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening, or violent comments about others, including the school staff, volunteers, governors, contractors, pupils, or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site, or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
9. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be found on the school wesbite and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
10. I can find out more about online safety at Belmont School by reading the full Online Safety Policy on the website and can talk to the class teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood, and agreed to this policy.

Signature/s: ____

Name/s of parent / guardian: ____

Parent / guardian of: ____

Date: ____

LGfL DigiSafe

Acceptable Use Policy (AUP) for EYFS/KS1 PUPILS

My name is ____________________

This is how I keep **SAFE online**: ✓

1. I only use the devices I'm **ALLOWED** to □
2. I **CHECK** before I use new sites, games or apps □
3. I **ASK** for help if I'm stuck □
4. I **KNOW** people online aren't always who they say □
5. I don't keep **SECRETS** just because someone asks me to □
6. I don't change **CLOTHES** in front of a camera □
7. I am **RESPONSIBLE** so never share private information □
8. I am **KIND** and polite to everyone □
9. I **TELL** a trusted adult if I'm upset, worried, scared or confused □
10. If I get a **FUNNY FEELING** in my tummy, I talk to an adult □

My trusted adults are:

____________________ **at school**

____________________ **at home**

Acceptable Use Policy (AUP) for
KS2 PUPILS

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework, and other activities to learn and have fun. I only use apps, sites, and games if a trusted adult says I can.
2. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people; I get creative to learn and make things!
3. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
5. ***I am careful what I click on*** – I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. ***I know it's not my fault if I see or someone sends me something bad*** – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell someone.
8. ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
9. ***I know new friends aren't always who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. If I want to meet them, I will ask a trusted adult, and never go alone or without telling an adult.
10. ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
11. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
12. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
13. ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
14. ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.

15. ***I am a rule-follower online*** – I know that apps, sites, and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.
16. ***I am not a bully*** – I do not post, make, or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
17. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
18. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures, or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
19. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

____

I _______________________________________have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes.

Outside school, my trusted adults are___________________________________

Signed: ________________________ **Date: ____________________**

LGfL DigiSafe

Acceptable Use Policy (AUP) for Staff/Governors/Volunteers

What is an AUP?

We ask all children, young people and adults involved in the life of Belmont School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations, and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy online.

Where can I find out more?

All staff, governors and volunteers should read Belmont School's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g., Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to any member of the Senior Leadership Team.

What am I agreeing to?

1. I have read and understood Belmont School's full Online Safety policy (see school website) and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult).
3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
4. I understand that internet and device use in school, and use of school-owned devices, networks, and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible, and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening, or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, that of the school and of the teaching profession), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in Belmont School's social media policy/guidance.
9. I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location, or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.
10. I agree to always adhere to all provisions of the school Data Protection Procedures, whether I am on site or using a school device, platform, or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share

credentials, and immediately change passwords and notify the Headteacher if I suspect a breach. I will not store school-related data on personal devices, storage, or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property, and copyright rules always.

11. I will use school devices and networks/internet/platforms/other technologies for school business, and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use" as defined by HM Revenue & Customs.
12. I will not support or promote extremist organisations, messages, or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download, or send material that is considered offensive or of an extremist nature by the school.
13. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
14. I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are unimportant – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handing incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.
15. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

<u>To be completed by the user</u>

I have read, understood, and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: ____

Name: ____

Role: ____

Date: ____

<u>To be completed by the Head teacher</u>

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems: ____

Additional permissions (e.g., admin) ____

Signature: ____

Name: ____

Role: ____

Date: ____

LGfL DigiSafe

Acceptable Use Policy (AUP) for Visitors/Contractors/Lettings

What is this document?

We ask all children, young people and adults involved in the life of Belmont School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media.

Visitors and contractors are asked to sign this document before they are allowed access to the school. Many of these rules are common sense – if you are in any doubt or have questions, please ask.

Where can I find more information?

Further details of our approach to online safety can be found in the overall school Online Safety Policy on the school website.

If I have any questions during my visit, I will ask the person accompanying me (if appropriate) and/or a senior member of staff.

What am I agreeing to?

1. I understand that any activity on a school device or using school networks/platforms/internet may be captured by one of the school's systems securities, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. If I am given access to school-owned devices, networks, cloud platforms or other technology:
    - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use.
    - I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role.
    - I will not attempt to contact any pupils/students or to gain any contact details under any circumstances.
    - I will protect my username/password and notify the school of any concerns.
    - I will abide by the terms of the school Data Protection Procedures.
3. I will not share any information about the school or members of its community that I gain because of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
4. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.

5. I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils/students and will not give any advice on online-safety issues unless this is the purpose of my visit, and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCCIS).
6. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff, or pupils/students. If required (e.g., to take photos of equipment or buildings), I will have the prior permission of the Headteacher (this may be delegated to other staff), and it will be done in the presence of a member staff.
7. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: ____

Name: ____

Organisation: ____

Visiting / accompanied by: ____

Date / time: ____