Belmont Preparatory School
Online Safety Policy

1 Introduction

1.1 ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

1.2 Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video, email and web functionality
- Other mobile devices with text, video, email web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Streaming
- Music Streaming

1.3 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

1.4 At Belmont Preparatory School we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.5 Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the School. This can make it more difficult for the school to use technology to benefit learners.

1.6 Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

1.7 Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) as included at Appendix 1 are inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc) and technologies owned by pupils and

staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

1.8 This policy has been written with regard to the legislation laid out in Appendix 5, as well as legislation laid out in the Safeguarding Policy. It is important to note that in general terms, an action that is illegal if committed offline, is also illegal if committed online.

2 Online Safety – Roles and Responsibilities

2.1 As Online Safety is an important aspect of strategic leadership within the school, the Headmistress and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Designated Safeguarding Lead (DSL) and Deputy DSLs (responsible for EYFS, Lower School and Online Safety) are responsible for carrying out this process. All members of the school community have been made aware of who hold these posts. It is the responsibility of the Deputy DSL for Online Safety to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The Deputy DSL for Online Safety will also carry out a regular audit of the online activity of members of the school community through the monitoring of the school filtering system.

2.2 All governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

2.3 This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding, Health and Safety, Behaviour and Discipline, Anti-bullying and Personal, Social & Health Education.

2A) Staff Professional Responsibilities

2.4 When using any form of ICT, including the Internet, in school and outside school, for your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies. Staff should be reminded that all school communication should be carried out using the school email system.

- Do not talk about your professional role in any capacity when using social media such as Facebook and Twitter.

2B) Breaches of Online Safety Policy

2.5 A knowing and intentional breach, or suspected breach, of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

2.6 Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

2.7 The Information Commissioner's Office (ICO) powers to issue monetary penalties came into force on 6 April 2010, allowing the ICO to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

2.8 The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act,
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period,
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law,
- Prosecute those who commit criminal offences under the Act,
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern.

2C) Computer Viruses

2.9 All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used.

2.10 Never interfere with any anti-virus software installed on school ICT equipment that you use.

2.11 If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Network Manager Tim Stannard immediately. The Network Manager will advise you what actions to take and be responsible for advising others that need to know.

2D) E-mail

2.12 The use of e-mail within schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette. The new National Programme of Study for ICT states that pupils must have experienced sending and receiving emails.

2.13 Managing e-mail:

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use their school email accounts on the school system and only under teacher supervision for educational purposes.
- Pupils have their own individual school issued accounts.
- Staff and pupils must inform the Headmistress if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the ICT Scheme of Work.
- Check your e-mail regularly, i.e. daily during term time. All e-mails must be responded to (even with a "holding" e-mail) by the end of the next working day.
- If appropriate to your role, activate your 'out-of-office' notification when away for extended periods.

2.14 Password and Password Security:

a) Passwords:

- Always use your own personal passwords.

- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to the Network Manager when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you are aware of a breach of security with your password or account inform the Network Manager immediately.

It is advised that:

- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.
- User ID and passwords for staff and pupils who have left the school are removed from the system within 24 hours. If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager.

b) Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy and Data Security.
- Users are provided with an individual network, email, learning platform and Management Information System (where appropriate) log-in username. They are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers or teachers. On-line materials held in shared areas are accessible.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Computers attached to the school's internet are automatically locked after a maximum 5 minutes of inactivity.

3 Online Safety in the Curriculum

3.1 ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.

3.2 The school has a framework for teaching internet skills in ICT lessons and provides opportunities within a range of curriculum areas to teach about Online Safety.

3.3 Educating pupils about the online risks that they may encounter outside school is done when opportunities arise and as part of the Online Safety curriculum.

3.4 Pupils are aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do, but also serves to protect them.

3.5 Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.

3.6 Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.

3.7 Pupils are taught about the dangers of Youth Produced Sexual Imagery - YPSI (previously known as Sexting). They are taught that creating, sharing and possessing sexual images and videos (even once) of under-18s is a criminal offence. Pupils are taught about the consequences of such action remaining on their "digital footprint" in perpetuity, which could have long-term consequences for further education and employment throughout their adult lives. This is covered through the PSHE curriculum in the Upper School and bi-annual presentation by an Online Safety Officer.

3.8 Our staff receive regular information and training on Online Safety.

3.9 New staff receive information on the school's acceptable use policy as part of their induction.

3.10 All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.

3.11 All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

3A) Managing the School Online Safety Messages:

3.12 We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.

3.13 The Online Safety policy will be introduced by class teachers and/ or form tutors to the pupils at the start of each school year.

3.14 Online Safety posters will be prominently displayed.

3B) Internet Access

3.15 The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use of the internet is detected it will be followed up.

3C) Managing the Internet

3.16 The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

3.17 Staff will preview any recommended sites before use.

3.18 Raw image searches are discouraged when working with pupils.

3.19 If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents check these sites the children are using and supervise this work. Parents will be advised to supervise any further research.

3.20 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

3.21 All users must observe copyright of materials from electronic resources.

3.22 Monitoring and Filtering of Online Access:

- All web traffic, whether from wired of WiFi devices including phones, at Belmont is routed through a hardware web filter which, based on a number of criteria, either allows or blocks access to the site the user is attempting to access.
- For devices which form part of the school network and devices connected via the "BYOD" WiFi network, different filtering policies are applied depending upon the users' login names.
- There are different policies for admin staff, staff, and pupils. Where a user is connected to the guest wifi network, a more limited "default" policy is applied.
- Sites are categorised and constantly updated by iboss and most filtering is achieved by blocking or allowing access to certain categories (eg Games, Adult, Gambling, Sex Ed) but we have the capability to override (either blocking or allowing) per site or domain.
- Every attempt to access websites, successful or failed, is logged and kept together with the username (if from a Belmont owned PC or BYOD), IP address of the device, date/time, category and whether the access was allowed of blocked.
- The Network Manager and Deputy DSL analyse these on a regular basis (usually weekly, but at least every two weeks) and where issues are identified, report to the appropriate member of staff. The Network Manager is informed immediately automatically via email of any persistent attempts to access blocked sites and reports this to the Deputy DSL.

- Further guidance on monitoring and filtering can be found at UK Safer Internet Centre https://www.saferinternet.org.uk

3.23 The school does not allow pupils access to internet logs.

3.24 If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported to the Deputy DSL with Responsibility for Online Safety and IT or teacher as appropriate.

3.25 It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

3.26 If there are any issues related to viruses or anti-virus software, the Network Manager should be informed.

4 Incident Reporting, Online Safety Incident Log and Infringements

4A) Incident Reporting

4.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected serious misuse of ICT must be immediately reported to your line manager.

4B) Inappropriate Material

4.2 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to Mr. John Stevens, Head of IT.

4.3 Deliberate access to inappropriate materials by any user will be reported to Mr. John Stevens, Head of IT or to the Deputy Head (Pastoral). Serious offences by pupils will be dealt with through the Behaviour Management Policy.

4C) Managing other Web2 Technologies:

4.4 Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

4.5 Pupils are not permitted to access social networking websites or online gaming sites whilst in school.

4.6 All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

4.7 Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online. Pupils are taught about the dangers of Youth Produced Sexual Imagery - YPSI (previously known as Sexting). They are taught that creating, sharing and possessing sexual images and videos (even once) of under-18s is a criminal offence. Pupils are taught about the consequences of such action remaining on their "digital footprint" in perpetuity, which could have long-term consequences for further education and employment throughout their adult lives.

4.8 Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/email address, specific hobbies/ interests).

4.9 Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

4.10 Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

4.11 Cyberbullying is not tolerated at Belmont. Any instances of cyberbullying must be reported to a teacher.

4.12 Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school Virtual Learning Environment.

5 Parental Involvement

5.1 We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. We will consult with parents to seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

5.2 Parents are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

5.3 Parents are required to make a decision as to whether they consent to images of their child being taken and used in the public domain.

5.4 The school disseminates information to parents relating to Online Safety where appropriate in the form of:

- Information evenings.
- Practical training sessions.
- Posters.
- School website
- Newsletter items
- Information leaflet 'Belmont Preparatory School ICT and Online Safety' attached as Appendix 2 and as 'Information for Parents' attached as Appendix 3.

6 Safe Use of Images and Film

6A) Taking of Images and Film:

6.1 With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

6.2 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless using school owned storage devices, e.g. SD cards. This includes when on educational visits.

6.3 Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission.

6.4 Pupils and staff must have permission from the Headmistress before any image can be uploaded for publication.

6B) Consent of Adults Who Work at the School

6.5 Permission to use images of all staff who work at the school is sought on induction and the consent form is located in the personnel file. A template copy of the form is attached to this policy as Appendix 4.

6C) Publishing Pupils' Images and Work

6.6 On a child's entry to the school, all parents/carers, as part of the Parental Contract, are asked to give permission to use their child's photos or images.

6.7 Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

6D) Storage of Images:

6.8 Images/films of children are stored on the school's network and secure cloud-based server.

6.9 Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

6.10 Staff have the responsibility of deleting the images when they are no longer required.

6E) Webcams and Closed Circuit Television (CCTV):

6.11 The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.

6.12 We do not use publicly accessible webcams in school.

6.13 Webcams in school are only ever used for specific learning purposes.

6.14 Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

6F) Video Conferencing and Use of Skype

6.15 Pupils may only take part in video conferencing or use Skype under the supervision of a member of staff.

7 School ICT Equipment, including Portable and Mobile ICT Equipment and Removable Media

7A) School ICT Equipment:

7.1 As a user of the school ICT equipment, you are responsible for your activity. ICT equipment issued to staff is logged by the Network Manager and a central record of serial numbers is kept as part of the school's inventory.

7.2 Visitors may not plug their ICT hardware into the school network points (unless special provision has been made by the Network Manager). They should be directed to the wireless ICT facilities if available.

7.3 Ensure that all ICT equipment that you use is kept physically secure.

7.4 Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

7.5 It is imperative that you save your data on a frequent basis to the school network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.

7.6 Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick, or other portable device. If it is necessary to do so the local drive must be encrypted. Encrypted memory sticks are available – contact the Head of IT.

7.7 It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.

7.8 On termination of employment, resignation or transfer, return all ICT equipment to the Network Manager or Head of IT.

7.9 It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

7.10 All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

7B) Portable and Mobile ICT Equipment:

7.11 This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

7.12 All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

7.13 Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.

7.14 Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

7.15 Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

7.16 Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

7.17 In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

7.18 Portable equipment must be transported in its protective case if supplied.

8 Bring your own device (BYOD) and access to the school network

8.1 Belmont operates a BYOD policy, whereby pupils in Years 2-8 are required to have tablet device for use within school. These devices are used to access a range of school learning areas: the VLE, ActiveLearn, PurpleMash. Pupils access prep and learning tasks through the VLE on a daily basis both within school and at home. Pupils are taught how to use and manage their devices effectively

8A) General Information:

8.1 Access to the Belmont Preparatory School wireless network, whether with school-provided or personal devices, is filtered in compliance with the Children's Internet Protection Act (CIPA). Pupils will only have access to documents which reside on the school network from their personal devices that are relevant to their learning. They

will only have access to their own personal file area and the common pupil area known as "GenShare".

8.2 Access to the Belmont Preparatory School wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the network also allows IT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request.

8B) Guidelines for Use

8.3 Use of personal devices during the school day is at the discretion of teachers and staff. Pupils must use devices as directed by their teacher.

8.4 The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. gaming, gambling or accessing social network sites is not allowed within school and contacting parents, should only take place after permission has been given from a teacher or other member of staff i.e. during boarding time if the child is a boarder. Pupils should ensure that every effort is taken to turn off notifications for messaging applications and disable those applications during the school day.

8.5 The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.

8.6 The use of personal devices falls under Belmont Preparatory School's Acceptable Use Policy.

8.7 Pupils shall not use personal devices outside of their classroom, e.g. break, lunchtimes or on the school minibus, unless otherwise directed by their teacher e.g. on school visits or activities.

8.8 Pupils shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

8.9 Pupils shall not create, store or distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

8.10 Pupils may not engage in personal attacks, harass another person, or post private information using text messaging, taking, sending or storing sexualised images (otherwise known as Youth Produced Sexual Imagery, previously known as Sexting) and phone calls. It should be noted that it is a criminal offence to use a mobile device to menace, harass or offend another person, as such the school may consider it appropriate to involve the police. The taking, sending or storing of YPSI is a separate criminal offence.

8C) Consequences for Misuse/Disruption (one or more may apply):

- Access to the wireless network will be removed.
- Device taken away for the period.
- Device taken away and kept in the school office until parent picks it up.
- Pupil is not allowed to use personal devices at school.

8.11 Serious misuse of Internet or other mobile technology capable devices is regarded as a serious offence within the School's Behaviour Management and Disciplinary Policies and will be dealt with in accordance with these policies. Where children under the

age of 13 are involved and the incident is deemed illegal or inappropriate then the school has a duty to inform the Local Area Designated Officer (LADO) and the police may be advised.

8D) School Liability Statement:

8.12 Pupils bring their devices to use at Belmont Preparatory School at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

8.13 Belmont Preparatory School is in no way responsible for:

- Personal devices that are broken while at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

8E) **Personal mobile devices (including phones)**

8.14 The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

8.15 Pupils are allowed to bring personal mobile phones to school but they must be switched off during the school day and handed in to their Form Teacher, the school office or Deputy Head (Pastoral).No mobile devices are allowed to be used while on a school minibus or trip, unless express permission has been sort and approved by a member of staff. Boarders are allowed mobile phones and these are stored during the school day in the Surgery.

8.16 The school is not responsible for the loss, damage or theft of any personal mobile device.

8.17 The sending of inappropriate text messages between any member of the school community is not allowed.

8.18 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

8F) School Provided Mobile Devices (including phones)

8.19 The sending of inappropriate text messages between any member of the school community is not allowed.

8.20 Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

8.21 Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

9 Social Media (including Facebook and Twitter)

9.1 Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

9.2 Our school office may use Facebook and Twitter to communicate with parents and carers.

9.3 Pupils should not have social media accounts, such as Facebook, SnapChat, Instagram or Twitter, as children under the age of 13 are not legally allowed to access these platforms. Pupils should be made aware that it is also their parents legal responsibility to ensure that they do no have access to these platforms.

9.4 Pupils are not permitted to access their personal social media accounts whilst at school.

9.5 Staff, governors, pupils and parents are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

9.6 Staff, governors, pupils and parents are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

9.7 Staff, governors, pupils and parents are aware that their online behaviour should at all times be compatible with UK law.

9.8 The school does not permit staff to accept as friends current pupils on a personal social network site.

Author:	John Stevens, Deputy DSL (Online Safety), Head of IT, Senior Tutor
Date:	September 2018 interim review
Approved by:	Safeguarding Committee
Date:	3 October 2018
Approved by:	Legal & Compliance Committee
Date:	20 November 2018
Review due:	Michaelmas 2020

APPENDIX 1:

Acceptable Use Policies:

EYFS and Lower School - Acceptable Use Agreement/ Online Safety Rules:

Dear Parents,

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr. Stevens, Head of IT.

- I will only use ICT in school for school purposes. I will not use my device whilst on a school minibus.
- I will only use my class e-mail address or my own school e-mail address when using school technologies.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

I know that my use of ICT can be checked and that my parents can be contacted if a member of school staff is concerned about my Online Safety.

Yours sincerely,

John Stevens
Head of IT

✂

We have discussed this and ..... (pupil name) agrees to follow the Online Safety rules and to support the safe use of ICT at Belmont Preparatory School.

Parent/Carer Signature .....

Form ..... Date .....

Upper School Pupils – Key Stages 2/ 3 - Acceptable Use Agreement/ Online Safety Rules:

Dear Parents,

ICT including the internet, e-mail, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of Online Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parents and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their Form Teacher, or Mr. Stevens Head of IT.

Please return the bottom section of this form to school for filing.

- I will only use ICT systems in school, including the internet, e-mail, digital video and mobile technologies for school purposes. I will not use my device while on a school minibus or on a school trip, unless direct permission is given by a member of staff.
- I will make every effort to ensure that all forms of messaging are switched off on my device during the school day and that my device does not receive notifications about those applications.
- I will not download or install software, or other executable files on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address when using school technologies and to communicate with teachers/staff at school.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address.
- I will not give out any personal information such as name, phone number or address.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without permission.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I understand that the consequences of taking, sending and storing Youth Produce Sexual Imagery may result in criminal proceedings against me.
- I understand that the use of devices to bully, humiliate, embarrass, threaten, cause offence to or degrade other pupils, staff or other members of the school community is unacceptable and that cyberbullying will not be tolerated in any circumstances and may result in criminal proceedings against me.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system, or try to gain access to staff-only areas of the network.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents may be contacted.

Yours sincerely,
John Stevens, Head of IT

✂

We have discussed this document and .....(pupil name) agrees to follow the e-Safety rules and to support the safe and responsible use of ICT at Belmont Preparatory School.

Parent/Carer Signature .....

Pupil Signature.....

Form ..... Date .....

Staff, Governor and Visitor Acceptable Use Agreement / Online Safety Rules and Procedures:

As part of the induction process, all new staff governors and visitors who have been provided with access to the school's network will be issued with the acceptable use agreement/code of conduct which they will be expected to sign. A copy of this will be kept on file.

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff, governors and visitors are aware of their professional responsibilities when using any form of ICT. All staff, governors and visitors are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with Rachel Eastment or Helen Skrine.

- I will use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes only.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role. All electronic communication with staff, parents and pupils will take place through the school email system.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will not accept as friends current pupils or past pupils of school age (i.e. Under the age of 18) on a personal social network site without the express permission of the Headmistress or Pastoral Deputy Head.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy on data protection and 'Safe Use of Images and Film' as set out in the Online Safety Policy. Images will not be distributed outside the school network without the permission of the parents and Headmistress, as outlined in the Data Protection Form signed by parents on joining the school.
- I will not use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless using school owned storage devices, e.g. SD cards. This includes when on educational visits.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online Safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School.

Signature: ..... Date: .....

Full Name ..... (Block Capitals)

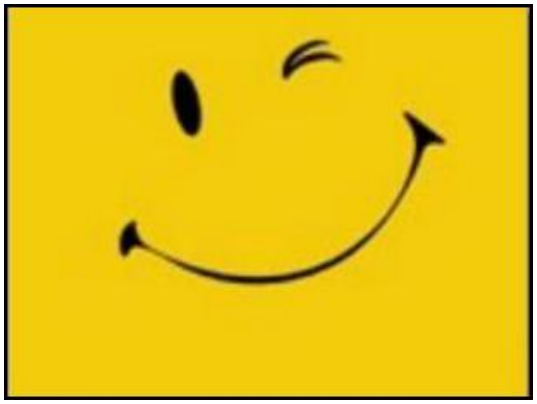
APPENDIX 2:

Belmont Preparatory School ICT & Online Safety:

Smile and Stay Safe Poster:

e-Safety guidelines to be displayed throughout the school

SMILE AND STAY SAFE



- Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.
- Don't reply to ASL (age, sex, location).
- Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.
- Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.
- Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.
- Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

APPENDIX 3:

Using the Internet safely at home:

Whilst many Internet Service Providers offer filtering systems to help you safeguard your child at home, it remains surprisingly easy for children to access inappropriate material including unsuitable texts, pictures and movies. Parents are advised to set security levels within Internet Browser with this in mind.

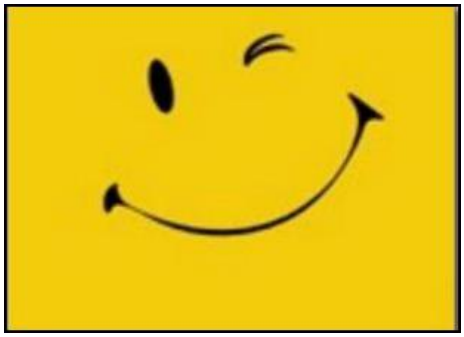
Locating the computer, tablet, or smartphone in a family area, will enable you to supervise children as they use the Internet. However, don't deny your child the opportunity to learn from the wide variety of material and games available on the Internet. Instead set some simple rules for keeping them safe and make sure they understand their importance.

Information for parents:

The purpose of this guide:

Children of today are increasingly using Information and Communication Technology (ICT) in schools and in the home. This guide explains:

- **S**afe
- **M**eeting
- **A**ccepting
- **R**eliable
- **T**ell



Simple Rules for keeping your child safe encourages young people to be **safe** by not giving out their personal details online draws attention to the risks associated with **meeting** someone you only know online highlights the risks of **accepting** emails, pictures and text messages from unknown sources is a reminder that not all information found online is necessarily **reliable** encourages children to **tell** someone if something happens or they meet someone online that makes them feel uncomfortable

Using these Rules:

Go through these rules with your child and you may like to pin these up near to the computer. It is also a good idea to regularly check the internet sites your child is visiting e.g. by clicking on History and Favourites.

- How your children are using ICT in school
- How using ICT in the home can help children to learn
- How children can use the Internet safely at home
- Where to access further information

Please reassure your child that you want to keep them safe rather than take internet access away from them

Some useful websites:

When searching the Internet we recommend you use one of the following child friendly search engines:

- Ask Jeeves for kids: www.askforkids.com
- Yahoo for kids: http://kids.yahoo.com/
- CBBC: http://www.bbc.co.uk/cbbc/find/
- Kidsclick: www.kidsclick.org

The following websites have useful information for parents and their children:

- The UK Safer Internet Centre: www.saferinternet.org.uk
- NSPCC NetAware: www.net-aware.org.uk
- Childnet: www.childnet-int.org
- Think U Know: www.thinkuknow.co.uk
- CEOP: www.ceop.gov.uk

How your child uses ICT at school:

ICT in schools is taught as a subject in its own right and also supports children's learning in other subjects, including English and mathematics. Within ICT lessons children learn to use a wide range of ICT including:

- Word Processing to write stories, poems or letters
- Databases to record information, e.g. minibeasts
- Spreadsheets to create tables, charts and graphs
- Desktop Publishing to design posters, leaflets or cards
- Multimedia Presentation to present text, pictures and sound
- Drawing Programs to create pictures and designs
- Internet to find information
- Email to contact children, parents and teachers within Belmont
- Digital Cameras to record what they have done in class or on a visit
- Electronic Sensors to record changes in light, sound and temperature
- Controllable Robots to give instructions and make something happen
- Simulations to explore real and imaginary situations

- Website Publishing to present ideas over the Internet

How you can help your child at home:

Benefits of using ICT at home:
ICT is not just about using a computer. It also includes the use of controllable toys, digital cameras and everyday equipment such as smartphones, iPads, mp3 and DVD players.

Children can be helped to develop their ICT skills at home by:

- writing a letter to a relative
- sending an email to a friend
- drawing a picture on screen
- using the Internet to research a class topic
- planning a route with a controllable toy
- using interactive games

How we know that using ICT at home can help:

Many studies have looked at the benefits of having access to a computer and/or the Internet at home. Here are some of the key findings:

- used effectively, ICT can improve children's achievement
- using ICT at home and at school develops skills for life
- children with supportive and involved parents and carers do better at school
- children enjoy using ICT
- using ICT provides access to a wider and more flexible range of learning materials

Social Media Platforms:

Belmont Preparatory School is committed to promoting the safe and responsible use of Facebook. Social Media such as Facebook, Twitter, Instagram and SnapChat offer amazing communication and social connections. However, Social Media and other forms of electronic communication, such as texting, can lead to problems (Youth Produced Sexual Imagery and grooming), when used irresponsibly at home or at school.

Facebook and other social media terms and conditions state that **all users must be 13 years or older**, so parents may wish to refer to the following points:

- Facebook use "age targeted" advertising (which may be of an inappropriate nature)
- Children may accept friends they don't know in real life
- Language and content is not moderated
- Underage users might be less likely to keep their identities private
- Facebook cannot and does not verify its members
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own

A selection of companies offer school software for use at home.

APPENDIX 4:

Use of Photographs and Other Images:

It is the custom and practice of most independent schools, and of this school, to include photographs or images of pupils and staff in the School's promotional material, such as the prospectus and website, and as a record of the life of the School for the enjoyment of the community and as part of academic work. Your consent to the use of such photographs and images is demonstrated by your signature on this form.

Name: .....

Signature: ..... Date: .....

APPENDIX 5:

Current legislation:

Acts Relating to Online Safety:

Racial and Religious Hatred Act 2006
It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk Communications Act 2003 (section 127) Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.

- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research

or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance -

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f76897/screening-searching-and-confiscation).

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent/carer to use Biometric systems.

The School Information Regulations 2012
Requires schools to publish certain information on its website –

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

The General Data Protection Regulations and UK domestic Data Protection Act 2018 (DPA).