Bexley Grammar School

E-Safety Policy

1. Rationale

Safe Internet use and the importance of being safe and responsible online are two of the most important principles for all members of our school community. The purpose of this policy is to set out the key expectations of all members of the school community at Bexley Grammar School with respect to the use of ICT-based technologies and to safeguard and protect both students and staff. It's important that we all work safely and responsibly with the Internet and other communication technologies and to monitor our own standards and practice. This document, and the related advice for students, staff and Parents/Carers, sets out clear expectations of behaviour relevant to responsible use of the Internet for educational, personal or recreational use. It clarifies the structures for Parents/Carers, students and staff that we have in place to deal with inappropriate online behaviours such as cyberbullying and sexting, linked to our Behaviour policy and ICT User Agreement. It clarifies to all members of the school community that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken. By clearly setting out the School's approach to e-Safety we will minimise the risk of inappropriate or malicious behaviour and the consequences that those behaviours can have.

2. Scope

This policy applies to all members of the Bexley Grammar School community (including staff, students, volunteers, Parents/Carers, visitors, community users) who have access to and are users of School's ICT systems, both in and out of School.

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 e-Safety behaviour that take place out of school. The school's Safeguarding Policy will also be referred to when dealing with Child Protection issues.

2.1 Research Data

According to the January 2014 Ofsted publication, 'Inspecting e-Safety in Schools' data compiled by OFCOM and other national surveys indicates that while children aged 5–15 continue to spend most time watching TV, children aged 12–15 are spending more time online (rising from 14.9 hours a week in 2011 to 17.1 in 2012) They are also more likely than they were in 2011 to mostly use the internet in their bedrooms (43% in 2012 compared to 34% in 2011). Over half of those aged 12–15 (55%). Children of all ages continue to use social networking sites; 22% of those aged 8–11 and 80% of those aged 12–15, with those aged 8–11 having an average of 92 'friends' and 286 for 12–15 year olds. Many incidents happen beyond the physical geography of the school gates and yet can impact on pupils or staff. 40% of Key Stage 3 and 4 students in the UK have witnessed a 'sexting' incident and, in the same group, 40% didn't consider topless images inappropriate. 28% of Key Stage 3 and 4 students have been deliberately targeted, threatened or humiliated by an individual or group through the use of mobile phones or the internet. Another national trend is that girls aged 12–15 are more likely than boys to say they have been bullied online in the past year (13% in 2012 compared to 5% in 2011). Supervising 'digital natives' can be difficult: forty–six per cent of Parents/Carers surveyed by Ofcom in 2012 agree with the statement: 'my child knows more about the internet than I do'. Agreement increases with each age group: 22% of Parents/Carers of those aged 5–7; 35% of Parents/Carers of those aged 8–11; and 67% of Parents/Carers of those aged 12–15. This national data makes it vitally important that pupils and staff are fully prepared and supported to use these technologies responsibly.

2.2 Policy Origins

This policy includes the views of pupils derived from a POWER Day solely dedicated to understanding how to be safe online and dovetailed with their ongoing PSHCE work. Parental liaison is also key to the successful implementation of the policy and the document has been approved by the PA as well as the Governing Body of the school. The attached guidance for staff has been produced in conjunction with several INSET sessions on dealing with e-Safety concerns and protecting their professional reputation. There is also attached guidance for Parents/Carers to read and consider when addressing e-Safety concerns and incidents with their children.

3. The main areas of risk for our School community

3.1 Content

Children are potentially the viewers, victims and creators of pornography today. We need to safeguard against this by monitoring and discussing their viewing and educating them about sex. Evidence suggests that children are increasingly aware of the physical side of sexual relationships but not the emotional, which is manifesting itself in violent and exploitative relationships. Problems include:

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

3.2 Contact

How do our children know who they are talking to? This is an issue from various perspectives:

- Child Sexual Exploitation;

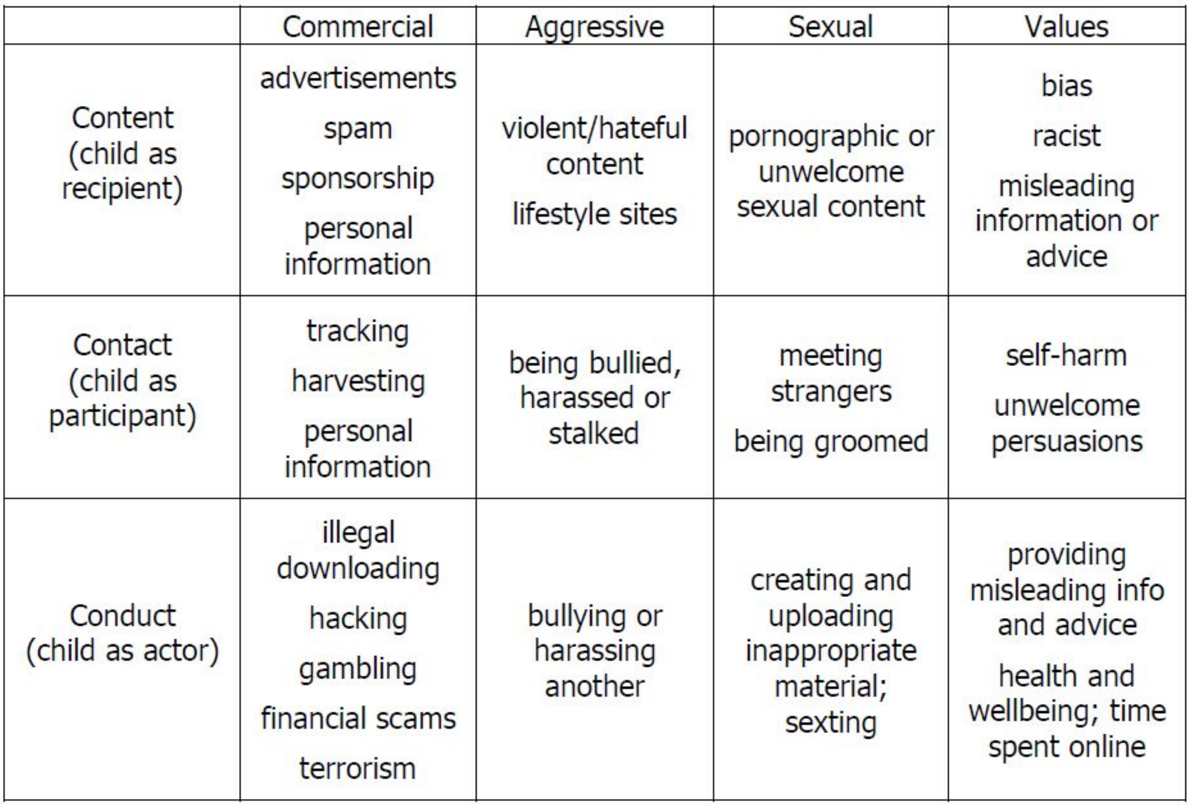
- Radicalization;
- Grooming;
- Cyber-bullying (please see the School's Anti-Bullying policy for guidance);
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords;

3.3 Conduct

Safe conduct online is appropriate for all members of the School community. The best advice for staff and students alike is do not do anything online that will cause harm to you or to others. Key problems include:

- Trolling (there is a sustained rise in online crime whilst 'real' crime drops);
- Privacy issues, including the disclosure of personal information;
- Your digital footprint and online reputation. What would an employer find out from a google search?;
- Mental health and well-being issues (linked to the amount of time spent online);
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- Copyright – children have little care or consideration for intellectual property and ownership (such as music and film);

3.4 Content, contact and conduct exemplars from Ofsted's 'Inspecting e-Safety in Schools' 2014



	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online

4. e-Safety Roles and Responsibilities at Bexley Grammar School

Role	Key Responsibilities
Headteacher	● To take overall responsibility for e-Safety provision ● To take overall responsibility for data and data security (SIRO) ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL ● To be responsible for ensuring that staff receive suitable training to carry out their e-Safety roles and to train other colleagues, as relevant ● To be aware of procedures to be followed in the event of a serious e-Safety incident ● To receive regular monitoring reports from the Designated Child Protection Lead ● To ensure that there is a system in place to monitor and support staff who carry out internal e-Safety procedures (e.g. network manager)
Designated Child Protection Lead	● To take day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school e-Safety policies / documents ● To promote an awareness and commitment to e-Safeguarding throughout the school community ● To ensure that e-Safety education is embedded across the curriculum ● To liaise with school ICT technical staff ● To communicate regularly with SLT and the designated e-Safety Governor to discuss current issues and incidents ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident ● To facilitate training and advice for all staff ● To liaise with the Local Authority and relevant agencies ● To keep regularly updated with e-Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ❖ sharing of personal data ❖ access to illegal / inappropriate materials ❖ inappropriate online contact with adults / strangers ❖ potential or actual incidents of grooming ❖ cyber-bullying and use of social media
e-Safety Governor	● To ensure that the school follows all current e-Safety advice to keep the children and staff safe ● To approve the e-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors Staffing and Pupil Welfare Committee receiving regular reports about e-Safety incidents ● To support the school in encouraging Parents/Carers and the wider community to become engaged in e-Safety activities ● The role of the e-Safety Governor will include:

	regular review meetings with the Designated Child Protection Lead
Computing Curriculum Leader	● To oversee the delivery of the e-Safety element of the Computing curriculum ● To ensure that all data held on pupils on the school's Learning Platform is adequately protected ● To liaise with the Designated Child Protection Lead regularly
Network Manager	● To report any e-Safety related issues that arise to the Designated Child Protection Lead ● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed ● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date ● To ensure the security of the school ICT system ● To ensure that access controls / encryption exist to protect personal and sensitive information held on School-owned devices ● To ensure that the school's policy on web filtering is applied and updated on a regular basis ● To ensure that LGfL is informed of issues relating to the filtering applied by the Grid ● To ensure that he / she keeps up to date with the school's e-Safety policy and technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant ● To ensure that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Designated Child Protection Lead / Headteacher for investigation ● To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster ● To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	● To ensure that all data held on pupils on the School Office machines have appropriate access controls in place
LGfL Nominated contact(s)	● To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
Teachers	● To embed e-Safety issues in all aspects of the curriculum and other school activities ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended School activities if relevant) ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff	● To read, understand and help promote the school's e-Safety policies and guidance ● To read, understand and adhere to the e-Safety policy's 'Guidance for Staff' ● To be aware of e-Safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices ● To report any suspected misuse or problem to the Designated Child Protection Lead ● To maintain an awareness of current e-Safety issues and guidance e.g. through CPD ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	● All new entrants to the school must read, understand, sign and adhere to the e-Safety Policy's 'Guidance for Students' ● To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology ● To know and understand school policy on the use of mobile phones, digital cameras and handheld devices ● To know and understand school policy on the taking / use of images and on cyber-bullying ● To understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school ● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home ● To help the school in the creation/review of e-Safety policies
Parents' Association / SMT link	● To liaise with and educate Parents/Carers on e-Safety issues ● To liaise with the PA regarding e-Safety issues pertinent to the wellbeing of the School Community
Parents/Carers	● To support the school in promoting e-Safety and endorse the Parents/Carers' guidance document which includes the pupils' use of the Internet and the school's use of photographic and video images ● To read, understand and promote the e-Safety policy's 'Guidance for Students' document with their children ● To read, understand and adhere to the e-Safety policy's 'Guidance for Parents' document ● To consult with the school if they have any concerns about their children's use of technology

External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

5. Communication

The policy will be communicated to Staff / Students / Parents / Carers community via the school website, the school's Staff Room and classrooms. New staff will be introduced to it during their Induction meeting. Students will have the school's ICT Acceptable Use agreements discussed with them at the start of each year and they will be held in pupil and personnel files.

All teaching staff are aware of the implications of the 2018 General Data Protection Regulation and have received appropriate training in this area. Please refer to the BGS Data Protection Policy, Privacy Notice for Pupils and Privacy Notice for Employees for further information.

6. Misuse and Complaints

Bexley Grammar School will take all reasonable precautions to ensure e-Safety is paramount and that staff and students act accordingly. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or that all incidents of misuse of the Internet can be addressed . Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Staff and pupils are given information about infringements in use and possible sanctions. Potential sanctions include:

- Interview by Tutor / Director of Study/ Designated Child Protection Lead / Headteacher
- Meeting with Parents/Carers
- Detention or Fixed-Term Exclusion
- Removal of Internet or computer access for a period
- Referral to Local Authority / Police.

Every incident is unique and we will treat individual circumstances differently. However if it is found that a student has clearly acted in violation of the e-Safety policy the matter will be dealt with by the Designated Child Protection Lead and the sanction deemed most appropriate will be applied.

Our Designated Child Protection Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to Child Protection are dealt with in accordance with school / Local Authority child protection procedures.

7. e-Safety Policy guidance for Pupils

7.1 Conduct and Safety

The best advice for all users of the Internet and social media is to STOP and THINK before you CLICK / TAP. Is this something that you would say to someone in person, or something that you would be happy for your friends/Parents/Carers/teachers to be aware that you were doing? Sensible and safe behaviour is about making good choices, whether it is online or offline.

The school's e-Safety policy relates to any actions that are linked to your membership of the Bexley Grammar School community. It's important that you adopt good e-Safety practice and act accordingly towards staff and other students.

Always follow the ICT Acceptable Use Agreement. Students are not permitted to use Internet enabled technology to access inappropriate content or to share such content with others, through their own accounts or the school network. The use of mobile technology to film or photograph students or staff without their permission is a serious breach of the behaviour policy and will incur sanctions. Misuse of the school network, either through a PC or by use of the school's Wi-Fi, will also lead to sanctions. If you are the victim of inappropriate ICT use, or you know someone who is, it's important that you inform a member of staff. Issues will be dealt with quickly and sensitively.

You should continue to behave acceptably when using an online environment/email, i.e. be polite, do not use bad or abusive language or other inappropriate behaviour. Cyberbullying, sexting and trolling are all things that can cause other people great upset and hurt. The use of mobile technology to harass other students or members of staff will be treated as a serious breach of school discipline and will warrant appropriate sanctions. Whether it is in the playground or an Internet forum, bullying / peer on peer abuse will not be tolerated at Bexley Grammar School. If you are affected by any form of online bullying speak to a parent or a member of staff. Don't allow it to continue.

Make sure that you are able to check and judge the accuracy of any information that you access online, including other people's profile details. Be aware that the author of a website/page/profile may have a particular bias or purpose for what they are doing, and they may not necessarily be trustworthy. Online 'friends' may not be who they say they are and you need to be careful in online environments: some people will 'groom' young people for sexual purposes.

Keep your personal information private; photographs can be manipulated and web content can attract the wrong sort of attention. Do not post or share detailed accounts of your personal life, such as contact information, daily routine, location, photographs and videos unless they can only be viewed by people that you know and trust. Do not post information or images that include the details of other people. Ensure that you have turned-on privacy settings and report abuse or suspicious contact on-line to a parent or carer, teacher, trusted staff member, Mr Gilmore or Mr Elphick. Organisations such as ChildLine, the NSPCC or the Metropolitan Police can also be contacted for advice or support.

Make sure you understand how a search engine works and how the results you see at the top of the listings are based on previous searches and access. Search results at the top of a page may well have paid to be there and might not be the most appropriate result. Many people and companies use the Internet to make money, through pop-ups, gaming / gambling sites, 'click bait' adverts or through phishing emails that attempt to get your personal details. Be aware of this when surfing the net and inform somebody from the list above if you encounter something odd or worrying.

When copying materials from the web, make sure you are aware of what plagiarism is and do not try to use other people's work as you own. Check copyright and acknowledge copyright/intellectual property rights. Do not download any files – such as music – without the permission of the owner. If in doubt regarding copyright law refer to the guidance received during Computer Science lessons or ask a member of staff.

Do not attempt to contact staff members through social media websites or to add them to user profiles. Any communication with staff should be conducted through the school's email system.

Do not take or post pictures or videos of others without their permission: you wouldn't like to have your privacy invaded by other people. Posting or forwarding inappropriate pictures or videos of other people is a crime and can lead to a police caution or worse.

7.2 Bring Your Own Device Policy (BYOD)

If you bring your own device to school you are responsible for its use and content. The school accepts no responsibility for loss, theft or damage of phones or tablets. Devices must be used appropriately and at teacher direction (Years 7-11) or in designated Sixth Form areas (Years 12 and 13), particularly regarding the recording, taking and sharing of images, audio and video. The school reserves the right to withdraw authorisation for the use of devices if at any time if it is deemed necessary and has the right to search the content of any mobile or handheld device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Mobile phones should not be used during the school day by Years 7-11 unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

If a mobile phone or device is found to breach the school's policy it will be confiscated and held at Reception until the end of the school day. If a student breaches the school's policy three times the phone will be kept on school premises until collected by a parent/carer.

7.3 Use of Email

All pupils are provided with an individual network log-in. It's your responsibility to make sure that your password is strong (a combination of unpredictable letters and numbers is a good start) and that anything accessed through your account is appropriate. You should not log on as another user (especially staff) and if you find a computer that has been left logged on you should log it out and log on again with your username and password. You should keep your password private and not make it accessible to others.

Everyone should be aware of the 'netiquette' of using email both in school and at home. Do not give out your email address unless it is to someone you know and trust and is approved by their teacher or parent/carer.

Email is a form of publishing where the message should be clear, short and concise. Any email sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper, as the communication is from a member of the School Community.

Do not reveal private details of yourself or others in email, such as address or telephone number. Try to 'Stop and Think Before You Click' to send, add or open attachments – if you have doubts it probably means that you shouldn't go ahead. It is not permitted to forward 'chain' email letters or to initiate one.

You must immediately tell a teacher / responsible adult if you receive an email which makes you feel uncomfortable, is offensive or bullying in nature. Do not respond to malicious or threatening messages but do not delete them immediately either - keep them as evidence of bullying or inappropriate contact.

Do not arrange to meet anyone that you meet online without having discussed with an adult and taking a responsible adult with you.

7.4 Health and Safety Considerations - advice from the Royal Society for the Prevention of Accidents

Using a computer is not generally thought of as being one of the most hazardous activities to engage in. Yet health and safety risks do exist for both adults and children. Here are some tips to minimise the risk of a computer-related accident:

- Site your computer near an electric socket to avoid trailing wires across the floor; if you use an extension cable make sure it doesn't overheat and nobody can trip over it
- Take care not to overload electric sockets; use trailing multi-socket units rather than plug adapters
- Always follow installation and service instructions in your computer guidebook closely. If in doubt, leave it to the experts
- Electricity and water do not mix - keep drinks and plants well away from computers
- Regularly check all electrical equipment for damaged plugs or frayed cables
- Computers are large and bulky pieces of equipment, move them only if you feel confident in doing so, and with care, especially up and down stairs. Use a trolley and a lift and ask for help.
- Do not play on or with computer swivel chairs
- Make sure the computer is sited in a position where you have plenty of room to move and to get out of the room in an emergency
- Organise workloads to avoid using the computer for extended periods of time
- Use your mouse as close to the keyboard as possible
- Adopt good posture while at the computer
- Know how to adjust your chair to the most comfortable position
- Minimise head and neck movements by altering the height of your monitor
- Regularly look at more distant objects, e.g. use thinking time to look out of the window, and take frequent breaks from computer work.

8. e-Safety Policy guidance for Staff

All staff in our school use technology to support and promote the learning and welfare of the children and as a school we are firmly committed to embracing the wonderful opportunities that the use of the Internet provides. However certain safeguards must be in place to protect all members of the School Community. It is the responsibility of all staff members to have read the school's e-Safety policy and associated documents. All members of the School Community are expected to be aware that misuse of the school's network to access inappropriate materials will have consequences. The Headteacher will have the final decision on whether a member of staff has behaved in an inappropriate or unprofessional manner constituting professional misconduct.

8.1 Mobile Phones and Devices

Staff members are responsible for the use and content of any mobile phone or device that is brought into school. The school accepts no responsibility for loss, theft or damage of phones or tablets. Devices must be used appropriately, particularly regarding the recording, taking and sharing of images, audio and video.

Staff must ensure that they do not give out their mobile phone number to students and do not contact children on the child's mobile phone either by voicemail or by texting unless in extreme circumstances and with the consent of the Headteacher, Safeguarding Lead or the Parent/Carer.

In the event that a staff member is required to use their own phone for school duties during an emergency they should safeguard their device by inputting 141 before their own number for confidentiality purposes.

In relation to photographs, staff must not use their personal mobile phone, camera or other devices to take, edit or store images of children from this school. In the event that mobile phones, cameras or devices are used to record images of children partaking in curriculum related activities the images should be downloaded onto the school's network before the mobile phone, camera or device is taken off site at the end of the school day and deleted from the device.

Staff should ensure that Bluetooth is disabled when on school premises on all personal devices, mobiles and laptops and not overshare information with students. It is strongly recommended that where possible mobile phones are password protected.

8.2 Email and Communication with Students

Communication by email should only be through the School's email system and personal emails must not be shared with children. Staff should not communicate with students through private email accounts or social networking accounts (even on educational matters) but must use official email for communication.

Sending emails that are not directly related to the student / teacher relationship and specifically relating to school business is deemed as inappropriate, as is the promotion of non-school activities such as outside clubs, events and organisations.

All staff members are provided with an individual network log-in. It's your responsibility to make sure that your password is strong (a combination of unpredictable letters and numbers is a good start) and that anything accessed through your account is appropriate. Passwords will need to be changed on a two-termly basis. You should keep your password private and not make it accessible to others. This applies to passwords used for access to all school related systems e.g. SIMS, Fronter etc.

Everyone should be aware of the 'netiquette' of using email both in school and at home. Email is a form of publishing where the message should be clear, short and concise. Any email sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper, as the communication is from a member of the school community.

Email correspondence of a personal nature should be restricted to a separate, personal email account and the address should not be used for professional matters.

Sensitive and personal data which requires data protection about a student should not be sent by email unless anonymised or encrypted. Child Protection issues, for example, should be communicated on paper or through private conversation.

In the event of an incident where data protection may have been compromised staff must report this immediately to the Headteacher or a Deputy Head.

8.3 Use of Social Media

Staff should be extremely careful in their personal use of social networking sites and ensure that profiles and accounts are set to the highest privacy settings and accessible only to trusted friends and family. These settings should be checked regularly to avoid loss of personal information.

Staff should not make reference to pupils, Parents/Carers or colleagues in their social media activity, nor should they discuss personal matters relating to members of the School Community when online. Personal opinions should not be attributed to the school or Local Authority.

Teachers should not communicate with students through social networks or allow them to access their social media spaces. Staff and student relations should take place through the school's preferred system. Communicating with students through Facebook or Twitter is inappropriate unless through a school approved forum e.g. the PE Department's Facebook Page.

Administration of all School approved social media sites (e.g. blogs, Facebook pages) should be password protected and run from the School website, with the staff member responsible for administering the site taking responsibility for its content and related activity.

Staff should take to care to protect their professional reputation when communicating with past students. Many will have social media profiles linked to current members of the student body and/or siblings currently at the school. All communications with former students are advised to take place through the BGS Alumni Facebook page or the Old Bexleians webpage.

8.4 Use of the Internet and School Account

Staff should not access or expose children or young people to unsuitable material on the Internet, and take care when searching for images 'live' in front of the class, for example. Staff must be mindful of the Teacher Standards when using the Internet in school and model high standards of safe and responsible behaviour in their use of technology during lessons.

Staff are responsible for the internet history of their account. It is advised that they do not leave a workstation unattended and always log off when they have finished working at one. Similarly any ICT equipment that is lent out by the school should be used appropriately and up to date anti-virus and spyware software should be installed. Any device, laptop or computer loaned to staff should be used solely to support professional responsibilities.

Staff should undertake a regular 'house-keeping' of their account, deleting digital materials and documents that are no longer needed from their area and the school's Shared drive and clearing their Inbox and Deleted Items folders.

9. e-Safety Policy guidance for Parents/Carers

In a recent Childline report, it was revealed that there was a 168% increase in the number of young people counselled in relation to online sexual abuse in 2013/14.

- Three quarters of this counselling was with young people aged between 12 and 15.
- 39% of 13-18 year olds know someone who has sent a sexual picture (sexting).
- 40% thought that a topless picture is fine.
- 15% thought that a nude picture is fine.
- It's estimated that 80% of self-generated child porn/abuse images are passed on and can be made widely available.

The Internet is removing the obstacles and inhibitions that children *used* to have and as their Parents/Carers, carers and teachers we have to work together to educate children in behaving safely and sensibly online.

The Bexley Grammar School e-Safety policy is not intended to inhibit young people or demonise the Internet. Online communication and research opportunities are an incredible means of enabling young people to learn. However, just as when the car first revolutionised transport, young people need to know how to be safe when accessing this fast-moving and potentially dangerous technology. Please read through the e-Safety policy and the linked guidance documents and discuss them with your child. If you would like further guidance, or to discuss the issues raised in person, please contact the school to arrange a meeting.

9.1 Common Misconceptions

We have a family computer and I check the history. It's fine.

The family computer is not the issue. Children can interact online through their phones, tablets, gaming machines, free gaming apps.

Yes, but we have the family filter switched on to all of our devices.

Filters have a 15% imperfection on overblocking and underblocking sites. Child Line was blocked until recently through one network filter. Worryingly 25% of Parents/Carers who have filters switched on see no need to discuss safe internet use with their children.

OK. But they are the digital natives. How can I possibly keep up?

The average 14 year old knows more about social media than the average 40 year old. But clearly we know more about making sensible decisions and dealing with mistakes effectively when they occur. This is why we need to teach them to be aware of the risks and to be resilient when accidents occur.

9.2 e-Safety Causes of Concern

This list is not exhaustive but includes many problems commonly encountered by children online.

- Oversharing of information
- Cyber-bullying / Peer on Peer abuse
- Viewing inappropriate content
- Racism
- Hacking and harvesting of personal information
- Inappropriate commenting e.g. Trolling
- Inappropriate contact
- Sexting
- Mental Health, Self-Harm, Anorexia and Suicide sites / blogs
- Grooming and Child Sexual Exploitation
- Radicalisation
- Gang culture
- Right-wing extremism

9.3 Websites of Note

Websites which potentially cause problems for children continue to emerge as the policing of them becomes more sophisticated. However these are ones that we are aware of as a school:

- Facebook – Over the last 5 years Facebook use by children has declined. How cool is something once your Parents/Carers are on it? However the ease with which fake profiles can be created remains a worry, and Facebook's policy of having an age restriction of 13 is not strictly enforced enough to deter children from joining.

- Tinder – A dating app linked to Facebook profiles. Worryingly more and more teens are creating profiles and using the app to talk to older people.
- Snapchat – Known colloquially as THE sexting app. Photos which are sent supposedly disappear after ten seconds. However they can be 'screenshot' to record a permanent image and sophisticated app software can be downloaded to 'absorb' the image onto the device which receives it.
- Instagram – Allows for the rapid upload and distribution of photos from a phone to various channels. Known as the most problematic for children quickly 'oversharing' information.
- Twitter – Popular for instant communication via a tweet. Often overused by children (and adults) who make inappropriate comments towards others.
- Tumblr – A micro blogging site that allows others to follow and discuss – known for anorexia and suicide 'support' blogs and picture uploading.
- ASK FM – This site is notorious for allowing users to register anonymously and post comments about a topic. It has been strongly linked to Cyber-bullying and the subsequent suicide of a child in the UK. Despite this it still has 150 million users.

Whilst the school acknowledges the many benefits that these social media sites and applications have we want Parents/Carers and children to be aware of the darker uses that they are employed for, and then make informed decisions about what is accessed and joined.

9.4 The Digital Footprint

THINK before they CLICK. Be it a post, a Tweet, an email, a Whatsapp message or a photograph children must be aware that what they upload can be a permanent record and representation of them online. Once something is 'out there' it is very difficult to take back: anyone who has access could have copied it for themselves, kept it for their own records or distributed it further. The boundaries that prohibited sexual, racist or aggressive behaviour have been removed by the Internet and children must understand that what they are saying or doing can be hurtful to others, and themselves. Many employers routinely view current or prospective employee's social networking pages: children of this generation of the almost unregulated Internet must be careful about what they say, post and divulge through their profile.

9.5 Sources of Guidance

Childnet International - A non-profit organisation working with others to help make the internet safe place for children.

Kidsmart - Also run by Childnet, this is designed to explain to young people how to stay safe online.

Childline - Supported by the NSPCC, this site contains useful advice to young people on a variety of issues that affect their wellbeing, including E-Safety.

CEOP: Child Exploitation & Online Protection Centre – Their website contains resources and advice for parents, students and professionals working with young people.

UK Safer Internet Centre – A source for e-Safety tips, advice and resources to help children and young people stay safe on the internet.

ChatDanger - This site explains how to stay safe in different forms of online chat including mobiles, internet messenger and gaming.

Families Matter – Extremism Online – A page of guidance for parents who are concerned about their child being radicalised by exposure to online materials.

9.6 Our Advice

Let's destroy the machines?

No. The Internet, and the wonderful benefits it brings, are going nowhere.

- Communicate with our children about their interests and what they are doing online.
- Monitor their computer use and access.
- Set clear boundaries about how much time is spent online, where and when.
- Discuss the problems that arise.
- Discuss with your child what is appropriate to upload and what is not.
- Check the privacy settings and parental controls on all of the devices that you have.
- Befriend your child on the sites that they use.
- Make sure that they know the facts about the things we sometimes find uncomfortable.
- Accept that the uncontrollable will happen and we have to deal with the outcomes.
- Ensure that children realise the importance of their digital footprint: it won't go away and so they need to engage and mould it.
- Work in partnership with school and other Parents/Carers.
- Check the school website for advice and updates.
- Check that relevant filters are applied to smartphones, devices and PCs.
- Encourage children to take responsibility for their actions and THINK before they CLICK.

10. Review and Monitoring

The e-Safety policy is referenced from within other school policies: ICT Acceptable User Agreement, Safeguarding / Child Protection policy, Anti-Bullying policy, the School Improvement Plan, Behaviour policy, Citizenship policy and the Spiritual, Moral, Social and Cultural policy.

The school's Designated Child Protection Lead who will be responsible for document ownership, review and updates. The e-Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. The e-Safety policy has been written by the Designated Child Protection Lead and is current and appropriate for its intended audience and purpose. There is widespread ownership of the policy and it has been agreed by the SMT and approved by Governors. All amendments to the school e-Safety policy will be discussed with all members of teaching staff.

11. References

Ofsted document Inspecting e-Safety in Schools 2013

LGFL e-Safety Policy Template 2015

SWGFL e-Safety guidance