BROOKE PRIORY SCHOOL

E-SAFETY POLICY 2022-23

Scope of this Policy
This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers. Both this policy and the Acceptable Use Policy cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

Introduction

It is the duty of Brooke Priory School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites
- Social networking sites
- Chat rooms
- Music/video downloads
- Gaming sites (in game purchasing)
- Online communities via games consoles
- Mobile internet devices such as tablets and smart watches
- Apps such as Tik Tok etc.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies. At Brooke Priory School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Roles and responsibilities

1. The Proprietor

The Proprietor of the school is responsible for the approval of this policy and for reviewing its effectiveness. They will review this policy at least annually.

2. DSL, Headmaster and the Senior Management Team

   The DSL has responsibility for online safety and is accountable to The Headmaster. He is ultimately responsible for the safety of the members of the school community.

   The Headmaster will ensure that:

   - staff, in particular the e-safety coordinator are adequately trained about e-safety; and
   - staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

3. E-safety coordinator DSL (Following KCSIE Guidance)

   The School's e-safety coordinator is responsible to the Headmaster for the day to day issues relating to e-safety. The e-safety coordinator, has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

4. Computing and IT staff

   The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the e-safety coordinator. This is done in partnership with the school's IT management, which is contracted to Mark1 IT.

5. Teaching and support staff

   All staff are required to sign the Acceptable Use Policy (on an annual basis) before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

6. Pupils

   Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused. The School will support parents/carers in issues relating to online safety/behaviours outside of school when appropriate.

7. Parents and carers

   Brooke Priory School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. Interactions and communication includes e-safety for parents evening and both hard copy and online copies of safer internet use information sent home. Parents play an equal role in educating children of the need to use digital devices and the internet in an appropriate and safe way.

Education and training

1. Staff: awareness and training

   New teaching staff receive information on Brooke Priory School's e-Safety and Acceptable Use policies as part of their induction. All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

   All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before using any technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

   Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

   A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's DSL. Cyber crime concerns will be referred to Cyber Prevent (East Midlands Police) by the DSL www.cyber4schools.net

2. Pupils: E-Safety in the curriculum

   IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it. The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise. At age-appropriate levels, and usually via PSHE, pupils are taught about their e-safety responsibilities and to look after their own online safety. From year V, pupils are informally taught about recognising online sexual exploitation (also covered in Science topic on Sex Education), stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL, Class Teacher or any other member of staff at the school.

   In year VI, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues. Pupils are encouraged to approach the DSL, parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents

   The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.
   The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges discussion

sessions for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

Policy Statements

1. **Use of school and personal devices**

Staff
School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them. Staff are required to use a two-step authentication method, including a use of password and code provided by a secure application. Staff at Brooke Priory School are permitted to bring in personal devices for their own use. Staff must ensure that their personal devices are switched to silent during the working day. They may use such devices only during break-times and lunchtimes, or in non-contact time in the staffroom or when off site. Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers. When contacting a parent by phone, staff will, where possible, use the school landline. In exceptional circumstances it may be necessary for a member of staff to use their own personal mobile (by inserting 141 pre-fix to withhold the number). Staff will have use of the school mobile phone for trips and visits. Staff will make no attempt to contact pupils or past pupils through use of any such device.

Pupils
School mobile technologies available for pupil use including laptops are stored in the trollies in the Library’s locked cupboard. Access is available via teaching staff. The school recognises that there may be occasions when the children are making use of this equipment unsupervised by a member of staff. The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with their class teacher to agree how the school can appropriately support such use. The class teacher will then liaise with the pupil's other teachers about how the device will be used at school.

Remote Learning (If necessary in the future)
During the Covid-19 pandemic, the school introduced home learning via Microsoft Teams. Staff used school laptops and pupils were given a Microsoft 365 account for use on a family device at home.

When live teaching, staff will;

- Look smart and professional
- Blur the background if necessary depending on where in the home you are teaching
- Not share inappropriate material
- Monitor pupil engagement and report to the DSL if there are any concerns

When remote learning, pupils will;

- Refrain from sending inappropriate messages to members of the class

- Respect the views and opinions of others by waiting their turn and putting up their hand or typing MIS

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made during break times, lunch time or noncontact time. When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school. Members of staff employed by Brooke Priory School must not be 'friends' with parents (unless previously friends or developed as a parental capacity), pupils or past pupils on any media.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored. Staff must immediately report to a member of the Senior Management team the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the DSL.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Brooke Priory School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should current school pupils be added as social network 'friends' or contacted through social media. Staff should exercise extreme caution when becoming 'friends' with past pupils on social media and should be able to justify why such 'friendships' are appropriate.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address for official School business. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils
There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. Pupils must report any accidental access to materials of a violent or sexual nature directly to the teacher in charge of the lesson who will inform the DSL. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. All internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system (Exa Networks). If this causes problems for school work / research purposes, pupils should contact the ICT Staff/Mark1 IT.

3. **Data storage and processing**
The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details. Staff and pupils are expected to save all data relating to their work to the school's central server. Personal staff devices, which are used to access emails, should be password protected.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. Classroom laptops are taken off site, however all data is saved centrally on the school server. Documents that are required off site are to be sent by the teacher to themselves using their school email. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the DSL.

4. **Password security**
Staff have individual school network logins, email addresses and storage folders on the server. Staff are regularly reminded of the need for password security. Pupils log onto the network using a generic profile. All members of staff should: · use a strong password (usually containing eight characters or more and containing upper- and lower-case letters as well as numbers), which need to be changed every 90 days; · not write passwords down; and · not share passwords with pupils or other staff.

Additionally, we use a two-step authentication login for staff e-mails to further protect sensitive information. Staff are also required to lock/log off their laptops when not in use.

5. **Safe use of digital and video images**
The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. When using digital images, staff should inform and educate pupils about

the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites). Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use, when appropriate, with the school outlining this at the start of the event. School will remind parents at each event either in writing on the programme or verbally that images taken should not be uploaded to social media.

The School makes use of an official photographer and videographer during productions and other whole school events to ensure the protection of pupils on the 'no photo' list. Video licences are always purchased for such performances.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy / IT Policy / EYFS Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
Pupils must not take, use, share, publish or distribute images of others. Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see BPS Consent for use of images letter- sent out to all parents on arrival at BPS). Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or social media platform, particularly in association with photographs.

In exceptional circumstances, it may be necessary for a member of staff to take a photograph on a personally owned device. In such cases, the school policy is that the image should be emailed to school or transferred onto the school server at the earliest convenience, and deleted from the device, in the presence of a colleague, within one week of the date taken.

6. Misuse

Brooke Priory will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy). The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

7. Social Media

We aim to minimise the risks to the School through use of social media by staff. It is designed to help staff use these platforms and services responsibly, to minimise the risks and to ensure consistent standards of use of social media.

A social networking site is any website, which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. It includes but is not limited to, sites such as Facebook, Snapchat, Instagram, Ping, YouTube, TikTok, Twitter and Wikipedia.

It is not intended to affect your ability to use social media such as twitter for purely professional purposes.

This policy applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff or any other IT equipment.

Breach of this element may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this element will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

Relationship with other School policies

If an internet post would breach any of our policies in another forum it will also breach them in an online forum. For example, staff are prohibited from using social media to:

- breach our acceptable use policy
- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Policy or related rules, policies and procedures;
- defame or disparage the School or our affiliates, parents, staff, pupils, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-Harassment and Bullying statement;
- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy;
- breach our Data Protection Policy (for example, never disclose personal information about a colleague, pupil or parent online);
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Behaviour online can be permanent and so staff must be extra cautious about what they say as it can be harder to retract.

Staff must also be aware of the particular risks to internet security that social media presents and so to comply within this policy, therefore must take any extra measures necessary not to allow any of their actions on social media sites to create vulnerability to any School systems, this includes the consideration of privacy settings on personal accounts.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

General rules for the responsible use of social media

Staff must be aware that their role comes with particular responsibilities and they must adhere to the School's strict approach to social media.

Staff must:

- ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives;
- obtain the prior written approval of the Headmaster, to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site;
- seek approval from the Headmaster before they speak about or make any comments on behalf of the School on the internet or through any social networking site;
- report to the Headmaster immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School or raises any safeguarding concerns about pupils within the School;
- immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy;
- consider whether a particular post puts their effectiveness as a teacher at risk;
- post only what they want the world to see.

Staff must not:

- provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School;
- post or publish on the internet or on any social networking site, any reference to the School, your colleagues, parents or pupils;
- use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;
- discuss pupils or colleagues or criticise the School or staff;

- post images that include pupils;
- harass or bully other members of staff;
- initiate friendships with pupils on any personal social network sites;
- accept pupils as friends on any such sites; staff must decline any pupil-initiated friend requests.

The use of social media for school purposes and in the School's name

Commented [HCR1]: Please see guidance note 12 (page 8 of the Handbook).

Social media should not be used for purposes relating to the School's business or the delivery of its curriculum to pupils unless the prior authority of the Headmaster has been obtained. Any breach of this restriction will be treated as a disciplinary matter. If you are permitted to use social media platforms in the School's name (this is currently limited to two members of the admin team), in addition to complying with the general rules above, you must also:

- clearly identify who you are, including your name and job title, and include contact details as appropriate as instructed by Headmaster
- ensure that all arrangements with any third party in relation to your use of social media (e.g. online advertising, search engine optimisation or other arrangements) are properly documented, notified and approved by [insert position];
- ensure that your use of the School's logos and other branding material is consistent with the School's relevant policies and procedures [and is approved by [insert position]];
- ensure that your communications are professional in tone rather than overly informal; and
- link back to the School's website as appropriate to highlight the School's offering.

Any social media accounts (including blogs, forums, twitter etc), sites or pages used or set up for the purpose of furthering the School's business or facilitating the provision of the curriculum to its pupils shall remain the property of the School and the designated leads must have access to it.

Personal use of social media

We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communication systems (including via smartphones and tablets). We authorise such occasional use [provided use is minimal and takes place substantially out of normal working hours (ie during your lunch break or before or after work) and] so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and is in accordance with this Policy.

Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the School's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

Permission to use the School's systems to access social media platforms for personal use may be withdrawn at any time at the School's discretion.

The monitoring of social media

The School's right to monitor, intercept and review communications applies equally to the use of social media platforms (and any postings and activities) made via the School's system or network. Any such monitoring will be for legitimate business purposes which include:

- ascertaining and demonstrating that our rules and being complied with;
- demonstrating that expected standards are being met by those using the systems; and
- for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for as long as is necessary for our legitimate business purposes in accordance with data protection law. We may delete such copies periodically or from time to time without notice when their retention is no longer necessary.

Do not use our IT resources and communication systems for any matter that you wish to be kept private or confidential from the School.

Social media and the end of employment

If a member of staff's employment with the School should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with the School.

All professional contacts that a member of staff has made through their course of employment with us belong to the School, regardless of whether the member of staff has made social media connections with them.

On the termination of employment for any reason, and when requested by the School at any time, staff will provide to the Headmaster any relevant passwords and other information to allow access to any social media site, page or account which has been used or set up for the purpose of furthering the School's business or facilitating the provision of its curriculum and will relinquish any authority they may have to manage or administer any such site, page or account.

Complaints

As with all issues of safety at Brooke Priory School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Headmaster in the first instance, who will liaise with the Senior Management team and undertake an investigation where appropriate. Please see the Complaints Policy for further information. Incidents of or concerns around e-safety will be recorded using an Incident Report form and reported to the school's Designated Safeguarding Lead, Joe Bancroft, in accordance with the school's Child Protection Policy.