BICKLEY PARK SCHOOL

E-Safety Policy

Policy Review & Update Process			
Member(s) of SLT responsible for update		Jonathan Poole	
Bickley Park School LAB responsible for review		Buildings, Health and Safety	
ISBA template policy?		Yes (modified)	
Last Updated	**September 2026**	Updated by	**JP**
Last review	**September 2025**	Next review	**September 2027**

Bickley Park School *(DfE number 305/6002) is a member of the* ***Sevenoaks Family of Schools*** *and a trading name of* ***Sevenoaks Education Group****, a company limited by guarantee (4908949) and a registered charity (1101358) with a registered office at Sevenoaks School, High Street, Sevenoaks, Kent TN13 1HU. Any reference to governors, the governing body, the proprietor or the chair of governors refers to the Sevenoaks Education Group Board. Any reference to local governors or local board refers to the non-executive members of the Bickley Park School Local Board.*

Contents

Introduction 3
Scope of this Policy 4
Roles and responsibilities 4
1. The Governing Body 4
2. Headteacher and the Senior Leadership Team 4
3. The Online Safety Officer 5
4. IT staff 5
5. Teaching and support staff 6
6. Pupils 6
7. Parents and carers 6
Education and training 7
1. Staff: awareness and training 7
2. Pupils: E-Safety in the curriculum 7
3. Parents 8
Policy Statements 9
1. Use of school and personal devices 9
Staff 9
Pupils 9
2. Use of internet and email 10
Staff 10
Pupils 11
3. Data storage and processing 11
4. Password security 12
5. Safe use of digital and video images 13
6. Misuse 14
Complaints 14

Introduction

It is the duty of Bickley Park 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;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- AI Generative tools
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the ICT Acceptable Use Policy, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Child Protection and Safeguarding;
- Staff Code of Conduct;
- Health and Safety;
- Behaviour Policy
- Anti-Bullying Policy;
- Social Media;
- Data Protection;

- Cameras and Mobile Phones Policy,
- EYFS Policy for use of Cameras and Mobile Phones
- Taking, Storing and Using Images of Children and
- PSHE.

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 Bickley Park 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.

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 ICT 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.).

Roles and responsibilities

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually. The Local Governor responsible for Safeguarding is also nominated as the Online Safety Governor, responsible for meeting with the school regularly.

2. Headteacher and the Senior Leadership Team

The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the online safety officer, Sarah Valero, the DSL, Jonathan Poole and the online safety group. The

online safety group comprises the Local Governor for Safeguarding and representatives from P365, who manage the schools IT.

In particular, the role of the Head and the Senior Leadership team is to ensure that:

- staff, in particular the online safety group, 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. The Online Safety Officer

The School's online safety officer is responsible to the Head for the day to day issues relating to e-safety. The online safety officer 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. 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 online safety officer.

The schools IT is monitored by P365 and they are responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any online safety policy / guidance that may apply
- users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- keeps up to date with online safety technical information in order to effectively carry out their online safety role and inform and update others as relevant
- the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head and Online Safety Officer for investigation / action / sanction

- monitoring software / systems are implemented and updated as agreed in school policies.
- **An annual review and risk assessment of our school system will be undertaken.**

5. Teaching and support staff

All staff are required to sign the ICT Acceptable Use Policy.

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.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school E-Safety Policy and practices
- they have read, understood and signed the Staff ICT Acceptable Use Policy
- they report any suspected misuse or problem to the Head and Online Safety Officer for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow this E-Safety Policy and the ICT Acceptable Use Policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the ICT Acceptable Use Policy and for letting staff know if they see IT systems being misused.

7. Parents and carers

Bickley Park 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.

Parents and carers are responsible for endorsing the school's ICT Acceptable Use Policy.

Education and training

1. Staff: awareness and training

New teaching and administrative staff receive information on Bickley Park School's E-Safety and ICT Acceptable Use policies as part of their induction.

All 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.

Commented [s1]: SM emailed JW to confirm process and ensure this is true

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. 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 via MyConcern or Confide as soon as possible if any incident relating to e-safety occurs and be notified directly to the school's online safety officer.

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 Computing 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 and Computing lessons, pupils are taught about their e-safety responsibilities and to look after their own online safety. Pupils can report concerns to the Head, the Online Safety Officer and any member of staff at the school.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Head, the Online Safety Officer as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and progressive and is delivered in the following ways:

- A planned online safety curriculum is part of Computing and PSHE lessons
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- As pupils progress through the school they are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- The school works to support pupils in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are taught responsible use of ICT through lessons and in line with the ICT Acceptable Use Policy
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites pupils visit
- It is accepted that, from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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 evenings 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.

Staff at Bickley Park School are permitted to bring in personal devices for their own use. They may use such devices in line with the school's mobile phone policy for their department: Camera and Mobile Phone Policy or EYFS Policy for Using Cameras and Mobile Phones.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils and under no circumstances should staff contact a pupil using their own personal telephone number, email address, social media, or other messaging system.

Staff are advised to be extremely cautious in conversations with other staff, parents and volunteers in social networking, including WhatsApp, on the basis that privacy laws can be violated even if a person's name is not shared. Staff should maintain a high level of professionalism in all communications with parents.

Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they must be handed in to the school secretary at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

No personal devices belonging to pupils are to be used at school, whether for school work or personal use.

School mobile technologies (iPads) available for pupil use are stored in allocated registration group locked cabinets. Access is available via the form teacher. These devices are for school use, both in school and at home. Pupils may take their device home to complete work set.

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 the SENDCO, to agree how the school can appropriately support such use. The SENDCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in staff-only areas of school.

This applies when teaching during the school term and when supervising children attending approved sports camps during the school holidays (and on school trips).

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.

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 the Online Safety Officer 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 Network Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Bickley Park 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 school pupils be added as social network 'friends' or contacted through social media.

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. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils in Year 2 and above are issued with their own personal iPad for use on our network and their own log in details for school networked devices. Access is via a personal login, which is password protected.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, pupils should contact Network Manager via their teacher for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff.

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 Online Safety Officer via their teacher. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded and will be dealt with under the school's Behaviour Policy. Pupils should be aware that 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. If this causes problems for school work / research purposes, pupils should contact the Network Manager, via their teacher for assistance.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy and the ICT Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their device or to the school's central server.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

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.

When personal data of staff or pupils is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Officer.

4. Password security

Pupils and staff have individual school network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and 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 should be changed every [6] months;
- not write passwords down; and
- not share passwords with other pupils or staff.

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. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the ICT Acceptable Use Policy / IT Policy / EYFS Policy / Taking and Storing Images of Children 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.

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 blog, particularly in association with photographs.

6. Misuse

Bickley Park School 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.

Complaints

As with all issues of safety at Bickley Park 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 Online Safety Officer, in the first instance, who will liaise with the Head 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 a Record of Concern entry on MyConcern or Confide and reported to the school's Online Safety Officer, in accordance with the school's Child Protection Policy.