

Online Safety Policy

This policy covers the Senior and Prep Schools and EYFS

Governors' Committee normally reviewing policy	Curriculum & Welfare
Date policy formally approved by Governors	September 2022
Period of review	1 Years
Last review date	August 2026
Next review date	August 2027

Person responsible for monitoring implementation and effectiveness of the policy	Deputy Head Pastoral
Other relevant policies	Pastoral Policies Safeguarding Policies

Kingsley School Bideford is owned and operated by KSI Schools Group Limited, which is the School's Proprietary Body ("the Proprietor").

Any reference in this policy to the Governors or Governing Body means the School's local body of governors, which operates as a local advisory board on behalf of the Proprietor. The local governing body does not constitute the Proprietary Body of the School.

The Proprietor has ultimate responsibility for ensuring that the School meets its statutory and regulatory obligations and for ensuring that this policy is appropriate, effective and implemented in accordance with those requirements.

The Governors provide local oversight and scrutiny on behalf of the Proprietor and undertake appropriate review and monitoring to satisfy themselves that this policy is being implemented effectively. They advise and make recommendations to the Proprietor and the School's leadership as appropriate.

The core principle that guides everything we do is **Putting Students First**.

1. Aims and Objectives

It is the duty of Kingsley School to ensure that every student in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use of IT Policy (for all staff, visitors and students), 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:

- Safeguarding and Child Protection Policy
- Radicalisation and Extremism Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy and Privacy Notice;
- PSHE / RSE Policy

The School understands the responsibility to educate students on online 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. The School understands the importance of involving students in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, students, 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 volunteers;

- “parents” includes students' carers and guardians; and
- “visitors” includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, 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 students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the “4Cs” outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many students will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some students, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by students, in or out of school, will be dealt with under the school's Behaviour Policy as is appropriate in the circumstances.

3. Roles and Responsibilities in Relation to Online Safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the Online Safety Lead, DSL, IT Manager and SLT are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2 Head

The Head is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Strategic Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3 The Designated Safeguarding Lead (DSL)

- i. The DSL takes the lead responsibility for Safeguarding and Child Protection. This includes a responsibility for online safety and for the school's filtering and monitoring system.
- ii. The DSL will ensure that this policy is upheld at all times, working with the Strategic Leadership Team, Online Safety Lead and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.
- iii. The DSL will work closely with the Online Safety Lead and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced.

The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

3.4 Online Safety Lead

The DSL has delegated day-to-day responsibilities relating to online safety to the school's Online Safety Lead. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Online Safety Lead will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL.

The online safety lead will:

- i. Complete an annual online-safety audit
- ii. Promote an online-safe culture under the direction of the SLT, and promote the School's online-safety vision to all stakeholders
- iii. Maintain the School's online-safety policy, reviewing it annually
- iv. Ensure that the online-safety policy links with other appropriate school policies e.g. Bullying Prevention, Safeguarding, PSHE etc. (with the appropriate members of staff)
- v. Ensure the online-safety policy and its associated practices are adhered to (e.g. incident flow charts, reporting logs etc.)
- vi. Ensure Acceptable Use Policies/school internet rules are in place, up-to-date and wherever possible are agreed by Staff, Students and Parents
- vii. Work with the SENCO and Designated Safeguarding Lead to create online-safety guidance for vulnerable children and those with additional learning needs
- viii. Manage online-safety training for all staff and ensure that online-safety is embedded within continuing professional development
- ix. Ensure staff receive relevant information about emerging issues
- x. Coordinate online-safety awareness raising/education for students and ensure that online-safety is embedded in the curriculum, for example via online-safety schemes of work, assemblies and/or theme days
- xi. Support online-safety awareness raising/education initiatives for parents
- xii. Act as a point of contact, support and advice on online-safety issues for staff, students and parents
- xiii. Act as the first point of contact should an online-safety incident occur (particularly child protection or illegal issues), and ensure the agreed online-safety incident procedure is followed, as outlined in the School's online-safety policy
- xiv. Maintain an online-safety incident log in CPOMS
- xv. Monitor, report and address incidences of students accessing unsuitable sites at school as necessary
- xvi. Keep up-to-date with local and national online-safety awareness campaigns and issues surrounding existing, new and emerging technologies

3.5 IT Staff

The school's IT 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 DSL, Online Safety Lead and/or Head of Prep School.

3.6 Teaching and Support Staff

- i. All staff are required to sign and return the Acceptable Use of IT Policy 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 online safety issues which may arise in classrooms on a daily basis.
- ii. All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL/Online Safety Lead.

3.7 Students

Students are responsible for using the school IT systems in accordance with the Acceptable Use of IT Policy.

3.8 Parents/Carers

The School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. The School regularly consults and discusses online safety with parents and seeks to promote a wide understanding of the benefits and risks related to internet usage. The School will contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

3.9 The Online-Safety Committee

- i. The Committee comprises of;
 - a. The online-safety lead
 - b. The designated safeguarding lead
 - c. IT manager
 - d. 1 member of SLT
 - e. 1 member of support staff
 - f. 1 member of residential house staff
 - g. 1 member of Prep School
- ii. The committee will meet once per term to review and share information about online-safety issues.
- iii. The Online Safety Policy will be reviewed annually

4. Filtering and Monitoring

In general:

The School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, students, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or

attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Lead will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding governor, the DSL and Online Safety Lead will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content and adult content. The IT Manager, DSL and Online Safety Lead will regularly add to the blocked content as needed. If there is a good educational reason why a particular website, application, or form of content should not be blocked a student should contact the relevant member of teaching staff, who will then contact the Online Safety Lead and DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Data Protection Policy and/or Privacy Notice/s, the Online Safety Lead/DSL/Deputy Head Pastoral/IT Staff will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the Online Safety Lead, the IT Manager and the DSL if they are teaching material which might generate unusual internet traffic activity.

5. Education and Training

- i. As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy. , all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.
- ii. All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures.
- iii. All teaching staff receive regular information and training (at least annually) on online safety issues, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. Support staff and contractors receive information about their responsibilities with regards to online safety during their safeguarding induction.
- iv. Teaching staff are encouraged to incorporate online 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. When students use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.
- v. In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.
- vi. The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, as well as informally when opportunities arise.

- vii. At age-appropriate levels, students are taught about their online safety responsibilities and to look after their own online safety. Students are formally and informally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Students can report concerns to any member of the pastoral team or using the online safeguarding reporting log.
- viii. Students are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Students are taught about respecting other people's information and images.
- ix. Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues. Students should approach their Head of Year, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

6. Use of School and Personal Devices

- i. 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.
- ii. Staff must not store images of students or student personal data on personal devices. Any taken must be uploaded to relevant social media posts or to the school system and then deleted from personal devices. *See Taking, Storing and Using Images of Children Policy.*
- iii. Boarders in Y7-11 must leave all personal devices except their laptops in their House during the school day.
- iv. If students Y7-11 bring in mobile phones (e.g. for use during the journey to and from school), they must be handed in to Reception at the start of the day and collected as they leave school. Prep children should hand their phones in to their Form Tutor. Mobile phones cannot be used during the school day (08:10-17:00). Sixth Form students may only use phones in the Sixth Form Common Room during break and lunchtimes.
- v. The school has introduced the use of student-owned laptops as a teaching and learning tool and students are required to adhere to the Acceptable Use of IT Policy when using their laptop for schoolwork. In particular, students must not use their laptop for non-school related activities during lessons.
- vi. Students are responsible for their conduct when using school issued or their own devices. Any misuse of devices by students will be dealt with under the School's Behaviour Policy.
- vii. The school recognises that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the SENDCO/Medical Team and Head of Year to agree how the school can appropriately support such use. The Head of Year will then inform the student's teachers and other relevant members of staff about how the student will use the device at school.
- viii. The school cannot be held responsible for the loss of, or damage to, any personal devices used in school or for school business.

7. Online Communications

- i. Any digital communication between staff and students or parents/carers must be professional in tone and content. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with students or parents / carers and recent alumni.

- ii. Staff must immediately report to the DSL / Head / Head of Prep if they receive 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 IT Manager.
- iii. All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure. Students should be aware that email communications through the school network and school email addresses are monitored.

8. Use of Social Media

- i. The school will control access to social networking sites, and consider how to educate students in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- ii. Use of video services such as Skype, Teams, Google Hangouts and Facetime will be monitored by staff in Residential Houses and provision will be made for Boarders to contact friends and family by these means.
- iii. Staff and students should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community. Any online communications, whether by email, social media, private messaging or other, must not:
 - place a child or young person at risk of, or cause, harm;
 - bring the 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.
 - otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

9. Data Protection

Please refer to the Data Protection Policy and the Acceptable Use of IT Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

10. Password Security

Students and staff have individual school network logins, email addresses, and storage folders on the server. Staff and students are regularly reminded of the need for password security.

All students 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 students or staff.

11. Safe Use of Digital and Video Images

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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 students about the risks associated with the taking, use, sharing, publication and distribution of images.
- The School will not publish private information to social media and websites.
- Written permission will be obtained from parents or carers in the Joining Pack before photographs or names of students are published on the school website or any school run social media.

12. Artificial Intelligence

The School is continuing to review AI tools and to educate staff and students on appropriate use. It cannot be used for any assessed work.

Please see the AI Policy for further details.

13. Misuse

It is appropriate for people to be allowed a great deal of freedom in using IT for study, work and leisure. With freedom comes responsibility. Kingsley School cannot control what people, all over the world, make available on the internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form.

We expect all IT users to take responsibility in the following ways:

- Not to access or even try to access any material which is:
 - Violent or that which glorifies violence
 - Criminal, terrorist or glorified criminal activity (including drug abuse)
 - Racist or designed to incite racial hatred
 - Of extreme political opinion
 - Pornographic or with otherwise unsuitable sexual content
 - Crude, profane or with otherwise unsuitable language
 - Blasphemous or mocking of religious and moral beliefs and values
 - In breach of the law, including copyright law, data protection, and computer misuse
 - Belongs to other users of IT systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's internet filtering
- Not to download or even try to download any software without the explicit permission of a member of the IT systems support department

- iv. Not to attempt to install any unauthorised or unlicensed software
- v. To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- vi. Not to use other people's user ID or password, even with their permission
- vii. Not to interfere with or cause malicious damage to the IT facilities
- viii. To report any breach (deliberate or accidental) of this policy to a member of staff immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. The School reserves the right to access all material stored on its IT system, including that held in personal areas of staff and student accounts for purposes of ensuring DfE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the IT facilities. The School will act strongly against anyone whose use of IT risks bringing the school into disrepute or risks the proper work of other users. Persistent offenders will be denied access to the IT facilities on a permanent basis.

14. Complaints

- i. Complaints of internet misuse will be dealt with in accordance with this policy.
- ii. Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- iii. Students and parents will be informed of consequences and sanctions for students misusing the internet in accordance with this and the behaviour policy.

15. Communication of the Policy

15.1 To students:

Students need to agree to comply with the student Acceptable Use of IT Policy in order to gain access to the school IT systems and to the internet

Students will be reminded about the contents of the Acceptable Use of IT Policy as part of their online-safety education

15.2 To staff:

All staff will be shown where to access the online-safety policy and its importance explained.

All staff must agree to comply with the staff Acceptable Use of IT Policy in order to gain access to the school IT systems and to the internet

All staff will receive online-safety training on an annual basis

15.3 To parents:

The school will ask all new parents to sign the parent /student agreement when they register their child with the school.

Parents' and carers' attention will be drawn to the Online Safety Policy in newsletters, and on the school website. Parents will be offered regular online-safety information.

K Venner

Deputy Head Pastoral