

Acceptable Use of IT Policy

This policy covers the Senior and Prep Schools and EYFS

Governors' Committee normally reviewing policy	Curriculum & Welfare
Date policy formally approved by Governors	November 2022
Period of review	1 Year
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 Curriculum 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. Scope of this Policy

This policy applies to all members of the school community (staff or students) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

2. Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- 2.1 The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- 2.2 Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- 2.3 Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- 2.4 Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- 2.5 Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- 2.6 Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

3. Using the School's IT Systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- 3.1 Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- 3.2 Do not attempt by any means (including the use of a Virtual Private Network (VPN)) to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- 3.3 Do not attempt to install software on, or otherwise alter, school IT systems.
- 3.4 Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

3.5 Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

4. Passwords

Passwords protect the school's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

5. Use of Property

Any property belonging to the school should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Manager.

6. Use of School Systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and students should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

7. Use of Personal Devices or Accounts and Working Remotely

7.1 Staff

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT Manager.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies.

7.2 Students

Students are expected to use their own device on the school system. They must sign the declaration below to confirm they have read this policy and agree to the terms of use.

8. Monitoring and Access

Staff, parents and students should be aware that school email, telephone system and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Personal devices used by students, whether or not such devices are permitted, may be confiscated and examined if there is any reason to suspect illegal activity or any risk to the wellbeing of any person. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

9. Tracking Devices and Technology

The school is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third party privacy considerations and only use it for domestic / personal purposes in respect of their own child and/or their or their child's belongings.

10. Compliance with Related School Policies

This should be read together with other relevant school policies.

11. Retention of Digital Data

Staff and students must be aware that all emails sent or received on school systems will be routinely deleted after 14 months and email accounts will generally be closed when a person leaves the school.

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or student file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the IT Manager.

Please see also the school's Privacy Notice.

12. Breach Reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;

- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or students become aware of a suspected breach, they must report it to a member of SLT and/or the IT Manager.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and students. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

13. Breaches of this Policy

A deliberate breach of this policy by staff or students will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Deputy Head Pastoral. Reports will be treated in confidence wherever possible.

14. Acceptance of this Policy

Users are expected to sign to 'accept' this policy on joining and revisited annually.

The Guest AUP must be signed by guests who are issued with a school guest-password to access the school network whilst visiting on-site.

K Venner
Deputy Head Pastoral

APPENDIX 1

Acceptable Use of IT Policy – Student Declaration - Senior

- i. I know that school owns the computer network and there are rules on how I use it.
- ii. I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner (the School).
- iii. I will only access the internet through the school Wi-Fi – I will not use a VPN or personal data
- iv. I will only use IT systems in school, including the internet, email, digital video, mobile technologies, etc., for school reasons. I will not use IT systems at school for private reasons, unless the Head has given specific permission. I will not use messaging apps (during the school day 0810-1700)
- v. I will not use IT systems at school to make money for me, gambling, political activity, advertising or for activities which are against the law.
- vi. I will only log on to the school network or learning platform with my own username and password.
- vii. I accept that I am responsible for all activity carried out under my username. I accept that I am responsible for all activity by my username.
- viii. I will follow the School's IT rules and not reveal my passwords to anyone and change them often.
- ix. I will only use my school email address for school work.
- x. I will make sure that everything I share, using the school network, with students, teachers or others is responsible and sensible. I know that emails might be shared with people I did not send them to.
- xi. I will not send messages without my own name or with a wrong name.
- xii. I will be responsible for my behaviour when I use the internet/learning platform. This includes resources I look at and the words I use.
- xiii. I will be polite and understand that other people might not think the same as me. I must respect their ideas and not be rude or disrespectful.
- xiv. I will not give out any personal information such as name, telephone number or address through email. I will not use the school IT to publish my personal ideas. I will not arrange to meet anyone unless this is part of a school project approved by my teacher.
- xv. I will not look at, download, upload or send on to anyone else material that could be offensive or against the law. If I accidentally come across any such things I will report it immediately to a teacher.
- xvi. I will not download or install software on the school network.
- xvii. I will not try to get round the school internet safety wall.
- xviii. I will make sure that my online activity, in school and outside school, will not cause my school, the staff, students or others to be upset or that it will not look bad for the school.
- xix. I will always respect that other people own their own work online and I will treat this as private to them.
- xx. I understand the school can check how I use the school's computer systems including websites I look at, emails I write and it might delete inappropriate work by me.
- xxi. I know that all my use of the internet and school's systems and other related technologies might be checked and staff told about what I do.
- xxii. I understand that these rules keep me safe and that if they are not followed, there will be sanctions and my parent/carers may be contacted. I understand that breaking the rules may result in the loss of my network or internet access.

For Tutors:

Name of Tutor _____

Tutor Group _____

I have read the Acceptable Use of IT Policy and agree to each of the statements on the Student Declaration:

[illegible]

Acceptable Use of IT Policy – Student Declaration - Prep

1. I will be kind and respectful

- ## 2. I will keep myself safe

- ### 3. I will use technology for learning

- 4. I will take care of equipment**

- 5. I will be honest**

- I understand that if I break these rules, I may not be allowed to use school devices or the internet for a while.**

Name of Tutor _____

Tutor Group _____

[illegible]

APPENDIX 3

Acceptable Use of IT Policy – Staff Declaration

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the online-safety coordinator.

- i. I appreciate that IT includes a wide range of systems, including mobile devices, tablets, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- ii. I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- iii. I will only use the School's email / internet / intranet / learning platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- iv. I will comply with the IT system security and not disclose any passwords provided to me by the School or other related authorities.
- v. I will not share the School's WiFi passwords with any students, staff, parents or visitors. I understand guests can access the Guest WiFi by signing the Guest Use declaration at reception where they will be given login information.
- vi. I understand that I am responsible for all activity carried out under my username.
- vii. I will only use the approved, secure email system(s) for any school business.
- viii. I will ensure that all electronic communications with parents, students and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- ix. I will ensure that personal data (such as data held on the school's MIS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- x. I will only take images of students and/or staff for professional purposes in line with school policy.
- xi. I will not install any hardware or software.
- xii. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- xiii. I will respect copyright and intellectual property rights.
- xiv. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.
- xv. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. I will support the School's online-safety policy and help students to be safe and responsible in their use of IT and related technologies. I will promote online-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. I will report any incidents of concern regarding children's safety to the online-safety coordinator, the Designated Safeguarding Lead or Head.
- xvi. I understand that sanctions for disregarding any of the above will be in line with the School's disciplinary procedures and serious infringements may be referred to the police.
- xvii. I understand that I may voluntarily declare the names of any persons under 19 years of age with whom I am in contact via social media, and that this information will be kept confidentially by the School.

Signed annually (or on joining) on the Staff Declaration and Details Form.

APPENDIX 4

Acceptable Use of IT Policy – Guest Declaration

- i. I understand that I have been given limited use of the school internet and/or school IT systems as a temporary guest user.
- ii. I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- iii. I will only use the school's email / internet / intranet / learning platform and any related technologies for the purpose for which I have been given access.
- iv. I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- v. I will not install any hardware or software.
- vi. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school IT systems.
- vii. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher or my employer.
- viii. I will respect copyright and intellectual property rights.
- ix. I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to the police.

Name

Company

Signed

Date