

| Policy: | IT Acceptable Use Policy | |
| --- | --- | --- |
| Applies to: | All pupils, staff and visitors at the College | |
| Owner: | Julian Noad, Head of College | |
| Reviews: | 22/6/22 JPN; 13/10/22 Governors (ESC); rewritten 5/1/23 by JPN to include staff (was just pupils) in line with ISBA; KFD 07/10/24 ISBA compliance; JPN 16/10/24 | |
| References: | ISBA [IT Acceptable Use Policy for Schools 23-10-2023.docx](https://docs.google.com/document/d/1bpXbtLqOdDT3wk8BJJGCO24VfgUV_qBd/edit?usp=sharing&ouid=100587920482851325768&rtpof=true&sd=true) | |

**Contents**

[1. Scope 3](#_gy4t1psj0j8e)

[2. Related policies 3](#_wxb8gn3s7ff9)

[3. Online behaviour 3](#_fgva5s7erl8j)

[4. Using the College's IT systems 4](#_3f69qynh3gm9)

[5. Passwords 4](#_efptk9oqitj9)

[6. Use of Property 4](#_h63i479masdf)

[7. Use of College systems 4](#_frmfudohci4f)

[8. Use of personal devices or accounts and working remotely 4](#_5t242np0b4ff)

[9. Monitoring and access 4](#_olcs7h85bbf7)

[10. Tracking Devices and Technology 5](#_ismida8tmdgr)

[11. Compliance with related College policies 5](#_yg6ebfaeuz7n)

[12. Retention of digital data 5](#_t6r0pyw4c9jw)

[13. Breach reporting 5](#_rhgr09sfp0dl)

[14. Breaches of this policy 6](#_afpk4gldeo6y)

[15. Acceptance of this policy 6](#_401jpvu5w37l)

### 

### **Scope**

* 1. This policy applies to all members of the College community (staff or pupils) who use College IT systems, as a condition of access. Access to College systems is not intended to confer any status of employment on any contractors.
  2. The College will take a wide and purposeful approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them.

### **Related policies**

* 1. [POLICY: Behaviour and Discipline](https://docs.google.com/document/d/14CEvReQmoy6UeQH-np9UFn8GL-fANhTnsYllQAkVdrk/edit)
  2. [POLICY: Anti-Bullying](https://docs.google.com/document/d/1ZB69UzlHtk-r4VZjcLfyHZT-nlYy7oAv4GZn-Mk1xLY/edit)
  3. [POLICY: Online safety](https://docs.google.com/document/d/1q0yacYegROXdiJPKAvsDNKOvD2x_Bvz_egUf1cNpSDE/edit)
  4. [POLICY: Child Protection & Safeguarding](https://docs.google.com/document/d/1rZzxeEzdCL4lHg0GYWrHOQ8t4Th8y48Imy73xDP3rus/edit)
  5. [POLICY: Child on Child Abuse Policy](https://docs.google.com/document/d/1pGmRSfhfOLzNh-dq0ZRi4KrWUantdYlDXKcCMO4kZTA/edit)
  6. [POLICY: Bring Your Own Device (BYOD)](https://docs.google.com/document/d/1CzD_HOiuHkiUzdKz9kRljkbZ-MKOfb9G-hW7oAahsag/edit?usp=drive_link)
  7. [POLICY: Taking, Storing and Using Images of Children](https://docs.google.com/document/d/15xssueFOGo0UF3jtUKtO-mpvdOezgpW2tF3MzddN7GY/edit)
  8. [Staff Use of Email, Internet, Communication Systems & Equipment Security Policy](https://docs.google.com/document/d/1cf6vbqYgZOi-UXbUCp986wf0aOPCcqrMLMuF0RecUwc/edit?usp=sharing)

### **Online behaviour**

* 1. As a member of the College community you should follow these principles in all of your online activities:
     1. The College cannot guarantee the confidentiality of content created, shared and exchanged via College 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. Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the College community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).

* + 1. Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the College community, even if the content is not shared publicly, without going through official channels and obtaining permission.
    2. Do not access or share material that infringes copyright, and do not claim the work of others as your own.
    3. 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.
    4. Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

### **Using the College's IT systems**

* 1. Whenever you use the College's IT systems (including by connecting your own device to the network) you should follow these principles:
     1. Only access College IT systems using your own username and password. Do not share your username or password with anyone else.
     2. Do not attempt to install software on, or otherwise alter, College IT systems.
     3. Do not use the College's IT systems in a way that breaches the principles of online behaviour set out above.
     4. Remember that the College monitors use of the College's IT systems, and that the College can view content accessed or sent via its systems.

### **Passwords**

* 1. Passwords protect the College’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. [This advice](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words) is helpful. 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.

### **Use of Property**

* 1. Any property belonging to the College 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 department.

### **Use of College systems**

* 1. The provision of College email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils 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 College's right to monitor and access web history and email use.

### **Use of personal devices or accounts and working remotely**

* 1. All official school business of staff and governors must be conducted on College systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for college purposes, and any removal of personal data or confidential information from college systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT department.
  2. Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the college's[POLICY: Bring Your Own Device (BYOD)](https://docs.google.com/document/d/1CzD_HOiuHkiUzdKz9kRljkbZ-MKOfb9G-hW7oAahsag/edit?usp=drive_link).

### **Monitoring and access**

* 1. Staff, parents and pupils should be aware that College email and internet usage (including through College Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and College email accounts may be accessed by the College where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.
  2. Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. 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, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

### **Tracking Devices and Technology**

* 1. 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.
  2. 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.

### **Compliance with related College policies**

* 1. To the extent they are applicable to you, you will ensure that you comply with the College's policies: [Behaviour and Discipline Policy](https://docs.google.com/document/d/14CEvReQmoy6UeQH-np9UFn8GL-fANhTnsYllQAkVdrk/edit), [Anti-Bullying Policy](https://docs.google.com/document/d/1ZB69UzlHtk-r4VZjcLfyHZT-nlYy7oAv4GZn-Mk1xLY/edit), [Online Safety Policy](https://docs.google.com/document/d/1q0yacYegROXdiJPKAvsDNKOvD2x_Bvz_egUf1cNpSDE/edit), [Child Protection & Safeguarding Policy and Procedure](https://docs.google.com/document/d/1rZzxeEzdCL4lHg0GYWrHOQ8t4Th8y48Imy73xDP3rus/edit), [Child on Child Abuse Policy](https://docs.google.com/document/d/1pGmRSfhfOLzNh-dq0ZRi4KrWUantdYlDXKcCMO4kZTA/edit), [Data Protection Policy](https://docs.google.com/document/d/1w_g2jxSrgAo-vdGDeftDqFpjxMHNJPZ3fMWy3DPLuxE/edit?usp=sharing), and [POLICY: BYOD](https://docs.google.com/document/d/1e1FpcUwkXJhpCXKsfll1BzoZ1cT7AbE2YGVXuduSqxs/edit)

### **Retention of digital data**

* 1. Staff and pupils must be aware that all emails sent or received on College systems will be handled as per the College’s [Privacy Notice](https://docs.google.com/document/d/173MmCSpWfOZ9PBL2Kzl0V8iJsRq00zfRArB8LspcsxI/edit#).
  2. Any information from email folders that is necessary for the College to keep for longer, including personal information (e.g. for a reason set out in the College privacy notice), should be held on the relevant personnel or pupil 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 College's email deletion protocol.
  3. 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 Department.

### **Breach reporting**

* 1. The law requires the College 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.
  2. This will include almost any loss of, or compromise to, personal data held by the College regardless of whether the personal data falls into a third party's hands. This would include:
     1. loss of an unencrypted laptop, USB stick or a physical file containing personal data;
     2. any external hacking of the College's systems, eg through the use of malware;
     3. application of the wrong privacy settings to online systems;
     4. misdirected post, fax or email;
     5. failing to bcc recipients of a mass email; and
     6. unsecure disposal.
  3. The College 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 College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.
  4. If either staff or pupils become aware of a suspected breach, please inform the Bursar or IT Manager who will, if appropriate log on GDPRIS, report to the ICO on behalf of the College and advise on next steps.
  5. Data breaches will happen to all organisations, but the College 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 pupils. The College'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.

### **Breaches of this policy**

* 1. A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter using the College's usual applicable procedures. In addition, a deliberate breach by any person may result in the College restricting that person’s access to College IT systems.
  2. If you become aware of a breach of this policy, or the [POLICY: Online safety](https://docs.google.com/document/d/1q0yacYegROXdiJPKAvsDNKOvD2x_Bvz_egUf1cNpSDE/edit), or you are concerned that a member of the College community is being harassed or harmed online you should report it to the IT Manager, Bursar or Head of College. Reports will be treated in confidence wherever possible.

### **Acceptance of this policy**

* 1. By using the College networks, you are consenting that you understand and agree to comply with this policy. A pop-up terms of service window will be displayed for pupils and staff on log-in for active user consent once per term. Guest users must verbally agree to the Acceptable Use Policy (AUP) before being granted access to the network**.**

**END**

