Biddenham International School & Sports College

ICT ACCEPTABLE USE POLICY

Introduction

The computer system is owned by the school, while 'Google Workspace for education' is a service provided by Google for the school. This Acceptable Use Policy aims to ensure that school ICT services, including Internet and cloud services are used effectively for their intended purpose, without putting users or data at risk and without infringing legal requirements.

This policy applies to all users of Biddenham School ICT facilities, both onsite and remote including Google Workspace. It applies to all accounts/devices connected to the school's ICT systems/cloud services/extensions. Steps must be taken to ensure the responsible use of all accounts/devices, including all personal devices, with the ability to connect to the schools ICT facilities.

Network Security

- Access to the school ICT systems must be through the user's own account and password provided by the school. Users must not share their usernames, passwords, or other login information with others or attempt to use another user's account (Even if they login for you). In certain situations Two Factor Authentication (2FA) will be implemented to add an additional layer of account protection to avoid unauthorised access.
- Internet content is filtered by the use of an external filtering company with an allow or block policy manually adjusted by the ICT Support Department. Whilst every effort is made by the filtering company, BISCC cannot guarantee that content inappropriate for the school environment is not accessible. No attempt should be made to probe or bypass the filtering system via any means. Doing so will result in sanctions being placed on the account and/or disciplinary action.
- Users with access to confidential data, for example student details, must take all possible actions to keep that data safe and confidential. Log off or lock must be made before leaving a workstation unattended. Hard copies must be destroyed (e.g. by shredding) after use. Removable storage media (e.g. USB flash drives) must be encrypted if containing sensitive data. Refer to the Cloud Services Policy for more information on storing data "in the cloud".
- It is the user's responsibility to make sure their user data is stored correctly so that it can be backed up. The school backs up SIMS and FMS data at least once per day; approximately six weeks of disk based backups are kept. With 12 Months of tape based backups being available as needed or for disaster recovery. All back-ups are held securely in a location separate from the master data and disk based online backups. Network drives are snapshotted twice daily with both full tape and disk backups taking place every other week with daily incremental backups also taking place to Disk and Replicated to tape.
- All data should be kept safe from viruses. All school ICT equipment has virus detection software installed which is regularly updated. Private equipment should have virus protection if the equipment is to be connected to the school systems for example through the wireless network access.
- Files which are restricted should not be downloaded by anyone other than the ICT Support Department. Restricted files include, but are not limited to, ones that end with: .EXE, .ZIP, .BAT, .COM, .INI.
- Only software owned or licensed by the school may be installed or used on school ICT systems; software must only be installed by the ICT support department (unless special permission has been granted for training or demonstration purposes).

Unacceptable Use

The school will exercise its right to monitor the use of the school's computer systems including access to websites and the interception/inspection of E-Mail or Google Docs. Where it believes

misuse of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes, storing unauthorised or unlawful text, imagery, sound, for the purpose of identifying a safeguarding/behavioural risk or concern. It may delete material or initiate disciplinary action (including restricting/denying access to the school's ICT systems) or report the misdemeanour to the appropriate authorities/DSL. Any violations of systems or network security are prohibited, and may result in the user being denied access to services, resulting in sanctions being placed on the account and/or being subject to school disciplinary procedure.

- Responsibility for all use of the school's computer system rests with each user. Workstations\Chromebooks must not be left logged on when the user is absent.
- Passwords cannot be shared. Passwords should be changed periodically in order to preserve security.
- In some cases 2FA will be implemented for additional security
- Any attempt to access, corrupt or destroy another user's data or to compromise the privacy of any user is unacceptable and is illegal under the Computer Misuse Act (CMA) 1990.
- The school's computer systems cannot be used for personal financial gain, for gambling, for political purposes, for advertising or to access or transmit pornographic or unlawful material.
- The school's computer systems must never be used for criminal activity. Breach of confidence, privacy or trade secrets is unacceptable.
- Users should never attempt to breach any technical safeguard, or to attempt to conceal their network identity, or to gain unauthorised access to any system or service.
- Copyright and intellectual property rights must be respected (the School has a CLA and ERA Licence which cover use of this material).
- It is a criminal offence to bully, menace, harass or offend another person. For example, the distribution of videos and pictures of an individual for public viewing without consent. As such you should not engage in any activity that could be considered harassment or cyberbullying using the school systems and report any such concerns to your HOY or line manager/grievance policy.
- All members of the school community should always conduct themselves in a polite fashion when using email, messaging, SMS or other forms of online communication. Anonymous, insulting, indecent, bullying, racist, sexist, homophobic, transphobic or any forms of hate speech messages, images or data are not allowed. Doing so goes against the Malicious Communications Act 1988 and can result in legal action.
- All students are taught how to keep themselves safe online. Unacceptable or suspicious behaviour or material must be reported immediately. Never disclose personal, financial, address or location details unless the user is absolutely sure of the trustworthiness of the recipient.
- Students in breach of acceptable use or conducting themselves in a negative light may have computer access/email access &/or internet access restricted or removed.
- Any staff authorised to access confidential data, for example student details, must take all possible actions to keep that data safe and confidential. This includes Locking\logging off before leaving a workstation, Processing data in a way that is expected ie. using school software/hardware rather than personal, destroying hard copies (e.g. by shredding) after use.
- School emails should not be forwarded to personal email accounts, (Sharing\Processing of sensitive\School data should be only be performed by authorised data controllers\sanctioned services)

Loss, Theft, and Damage

- BISSC accepts no responsibility for personal equipment brought onto the site.
- Excessive intentional damage will incur a repair cost up to the value of the replacement parts

or Chromebook.

- When a Chromebook is taken home appropriate physical security should be maintained to prevent loss, damage or theft.

Staff Communication with Students

- Communication between students and adults by whatever method should take place within clear and explicit professional boundaries.
- Adults should not request or respond to any personal information from a child or young person other than that which might be appropriate as part of the professional role. Adults should also ensure that all communications are transparent and open to scrutiny and made via official channels e.g. school email system.
- Staff should not give their personal contact details to students (including email, home or mobile telephone numbers) unless the need to do so is agreed with the Principal and the parent or carer of the child or young person. Inappropriate communication between an adult and child or young person outside the agreed protocols may lead to disciplinary and/or criminal investigation.
- Ensure that personal and social networking sites are set such that students are never listed as approved contacts.
- Never access or use social networking sites of students (except with the agreement of the designated member of staff).

Use of Social Media

- When using social media and internet sites the School draws no distinction between professional conduct online and offline.
- When using social networking sites and the internet staff should ensure that this does not damage the reputation of the School (or themselves) whether this is carried out during the school time or privately. Staff are personally responsible for the content they publish on social media sites and the internet and must be mindful that this information will be in the public domain. Employees must have regard to the fact that they will be responsible for any commentary which is deemed to be a breach of copyright, a breach of confidence, defamatory, libellous or obscene.
- Where appropriate, it should be clear that any views shared are the employees as an individual and not necessarily the views of the School.
- Any member of staff contacted by the published media or radio or television about a post they have made on a social networking site should inform the Principal immediately.
- No member of staff should use social media while in class with students (with the exception of school sanctioned accounts, e.g. departmental twitter/Instagram).
- Social media websites should not be used by parents to fuel campaigns and complaints against the school, or about members of the school community. Any concerns should be made through the appropriate channels by speaking to staff, the Principal or the Chair of Governors.

Password security and best practice are part of the supporting document ‘School Password Policy’.

Date of Next Review: **December 2024**