Bishop Justus School Policies

Policy Title:	Acceptable Use of ICT - Students
LT Responsibility:	Headteacher
Date:	October 2019
Review:	October 2021

RATIONALE

Bishop Justus Church of England School (the School) recognises the importance of Information Computer Technology (ICT) in enhancing the educational environment in which our students study. We understand the need to be ICT literate in order to live in the modern world; however we expect our students to understand the implications of ICT in working life and society and to respect the School's ethical, moral, spiritual and social values in the way ICT is used and what it is used for.
The purpose of the policy is to outline the acceptable use of ICT equipment for students at the School. It has been put in place to protect the School, staff, students and Aquinas Advisory Council from illegal or damaging actions by individuals either knowingly or unknowingly.
The policy applies to **ALL** student users of the School network; whether they are using ICT equipment owned or leased by the School, or using private equipment authorised to be connected to the School network. ICT facilities are provided for the educational benefit of students, and any behaviour that interferes with this will be considered an infringement of the policy.
A summary of the policy is contained in the student planner. This should be signed by the student and their parent/guardian to demonstrate their acceptance of the policy. Access to the School's ICT equipment will **NOT** be granted until this is completed.

ROLES AND RESPONSIBILITIES

Students have a responsibility to ensure that they use the ICT equipment in school or relation to the school in accordance with this policy. They must pay close attention to e-safety briefings given through assembles or during IT lessons.
The **Head of School** has a duty to ensure that students are safe when using the ICT equipment in school or in relation to the school in a safe manner.
The **Network Manager** has responsibility to ensure that students only have access to safe materials through the school network.

POLICY GUIDELINES

DATA PROTECTION & PROPRIETARY INFORMATION

The school uses data relating to students in accordance with the Data Protection Act. Whilst the School desires to provide a reasonable level of privacy, students should be aware that any data they create on the School systems remains the property of the school. The School reserves the right to

randomly check the contents of any computer or any storage media that may be connected to the School systems including USB flash drives (and CDs, DVDs, MP3 players, i-pods, mobile phones, smart phones and smart watches 6th form only). Any unsuitable material will be deleted and suitable disciplinary action taken.

Student data is collected to enable staff and support agencies to provide a high quality of education and ensure student support and extension is targeted correctly. Student's performance data is communicated to parents/guardians through regular assessment and reporting opportunities.
All School, student and staff details (including images and logos) are considered to be confidential and should not be disclosed to third parties without the express permission of the Head or Deputy Head Teachers and the IT Director.
Copyright of materials and intellectual property rights must be respected at all times. Students must **NOT** use or copy copyrighted material; including the digitization and distribution of photos from magazines and books, copyrighted music or logos.

SECURITY & SAFETY

Every student will be given an individual password to access the ICT systems, which will prompt students to change them every 60 days. Students **MUST** keep these passwords secure and not divulge or share them with others. All machines should be secured by logging off when students have finished using them. If at any time a student is not going to be in front of the machine they are logged into then they MUST logoff for security reasons.

Under no circumstances should you use iPhoto on a school Mac with an external storage device (phone/watch/ usb stick/ memory stick or hard drive) unless you are the logged on user. When you use iPhoto on a school Mac with an external storage device your images are automatically downloaded into the logged on users images folder. If you are not the logged on user then you are committing an offense against this school policy.

The School uses an up-to-date approved anti-virus software application to prevent the accidental transfer of viruses onto the network. As such, any storage media that is connected to the School network will be accessed and checked for viruses, with any infected files being deleted. Students should immediately inform their teacher or the IT Support staff if they are in any doubt.
Access to the internet is purely for educational purposes, and the School uses an approved web-filtering service to prevent access to unauthorised sites and to track internet usage. Students must **NOT** attempt to access sites for gambling or personal financial gain or that contain illegal images, political incitement, or promote religious or racial hatred or those that seek to undermine fundamental British values.

Any attempt to circumnavigate the anti-virus software or internet filters will be considered a serious infringement of the policy, and the appropriate disciplinary action will be taken. Students should be mindful of the Computer Misuse Act 1990, which criminalises any attempt to hack systems or knowingly introduce viruses.

Students will have access to E-Safety lessons during their ICT curriculum time and through year assemblies (see separate E-safety Policy).

EMAIL

Pupils may only use the approved email account for school purposes. Pupils must immediately tell a designated member of staff if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult. Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as has been approved by the Senior Leadership Team.

SOCIAL NETWORKING & CHAT SITES

The school will control access to social media and social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. Students must **NOT** publish details (including images and logos) relating to the School, students or staff on such sites without the express permission of the Head of School or Deputy Head Teachers and the IT Director. Any comments made on such sites relating to the School, students or staff must **NOT** be of a defamatory nature or damage the name or reputation of the School.

Students are not allowed to approach staff via social networking or chat sites. Any attempt to do so will be dealt with in school disciplinary sanctions imposed. Where students have intimidated or bullied others using social networking or chat sites (such as Facebook, Twitter, Instagram, Snapchat, BBM or MSN), this may be used as evidence where relevant to inform appropriate sanctions for further incidents of bullying, intimidation or aggression within school. Where material that brings the School into disrepute is posted onto social networking and self-broadcasting sites such as YouTube, the student posting it will remove it immediately under supervision within school, parental contact will be made by the School and sanctions issued.

FILTERING

The school's broadband access will include filtering appropriate to the age and maturity of pupils.
The School filtering system will block all sites on the Internet Watch Foundation (IWF) list. The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) should be aware of this procedure.
The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The School therefore cannot accept liability for the material accessed, or any consequences resulting from Internet use.

DAMAGE TO ICT EQUIPMENT

The ICT equipment provided by the School must be used sensibly and appropriately so as not to cause damage. Students will be responsible for the equipment they are using during the lesson until it is returned to the teacher. Any damage that occurs during this time will be repaired and the cost or such repairs will be billed to the parents/guardians of the student, unless the damage can be shown to be the fault of another student.
Any equipment that is found to be faulty at the start of a lesson should immediately be reported to the teacher or the IT Support staff.

ENFORCEMENT

Students will have their access rights reduced if they fail to adhere to this policy. This will range from the withdrawal of rights to use ICT equipment for the given lesson to the removal of rights for a specified period. The severity of any actions, including exclusion will be dependent upon the nature of the offence, and where appropriate the police or local authorities will be involved.
Any student that has their access rights removed will be given alternative paper based tasks that will allow them to continue to access a full curriculum entitlement.

CYBERBULLYING

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on Anti-bullying and Behaviour Management. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded.

USE OF PERSONAL ELECTRONIC ITEMS

Personal ICT equipment including personal laptops, smart phones, smart watches, android tablets and i-PADs may be connected to the school network with the permission of the school by 6th form students in the study centre only, using passwords distributed by the IT support staff. There is extensive provision for the taking of photos using school owned equipment which should be used at all times unless expressed permission by a staff member has been granted during a lesson.

For students in years 7-11, personal electronic items such as mobile phones, smart phones, digital cameras, MP3 players/i-PODs, i-PADs or laptops must not be used in school. These items will be confiscated if seen by staff members during the school day. There is extensive PC, Mac and Laptop provision for using the internet or software applications to aid study and the taking and storing of photos to enhance school work.

Bishop Justus Church of England School processes personal data in accordance with the data protection principles embodied in the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Academy complies with the requirements of the data protection legislation as detailed in the Trust Data Protection Policy.

All staff are aware of the principles of data protection and will not process personal data unless necessary. The Academy safeguards the personal data it collects through the operation of the Trust's data protection policy and processes and the IT policy. In addition, the Academy has taken steps to ensure that all its contracts that process data have the GDPR compliant provisions.

Signed:

……
Simon Murphy
Headteacher

Appendix A

Independent Learning
ACCEPTABLE USE POLICY

The school has installed computers, the Internet, software and other resources to help students' learning.

The following rules will help keep everyone safe when using these resources.

- Students will report any computer faults they find immediately to a member of staff.
- Students will treat the ICT resources with respect, leaving them as they would expect to find them.
- Students must ask permission from a member of staff before using ICT resources.
- Students will use only their own log in name and will keep their password a secret. Students will not access other people's files.
- Students may use the school's ICT resources ONLY for schoolwork.
- Students may only send email to people authorised by their teacher. Emails sent from school must be polite and sensible.
- Students may not disclose their personal details (such as their phone number or address), or the personal details of anyone else whilst using the Internet.
- Students should tell a member of staff about anything they see on the computer, which they are unhappy about, or if they receive messages which they do not like.
- The school reserves the right to check and monitor the contents of personal directories and to keep a check on Internet sites visited by students.
- Students are responsible for the contents stored in their personal area.
- Sharing of distribution of inappropriate files will receive a strong sanction.
- Students are responsible for checking ShowMyHomework to ensure all homework is completed.

PARENT/GUARDIAN'S SECTION
I have ensured that my son/daughter/guardian has read and understood the "Acceptable Use Policy" and that they understand its importance.

Signed:……. Date:…….

STUDENT SECTION
I have read and understood the "Acceptable Use Policy" and agree to abide by it whenever I am using ICT resources provided by Bishop Justus School.

Signed:……. Date: ……

Appendix B

HOW WILL E–SAFETY COMPLAINTS BE HANDLED?

Parents, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. E-Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.
A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e–Safety Coordinator. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Bromley Police Safer Schools Partnership Coordinator responsible for the school or the Children's Safeguard Team.

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.