

**STAFF ACCEPTABLE USE POLICY**

**THIS POLICY APPLIES ACROSS ALL TRUST SCHOOLS AND SERVICES**

|  |
| --- |
| **Document Management:**  Date Policy Approved: March 2014  Date Amended: August 202 4  Next Review Date: August 2027  Version: 4.0  Approving Body: Finance & Resources Committee |

|  |  |
| --- | --- |
| **Change Log** | |
| **Update:** | This Policy was updated to reflect the requirements of the Trust’s Online Safety, Social Media and Information Security Policies. It reflects the requirement for staff to complete Data Protection and Cyber-Security training. |
| **Location:** | Highlighted throughout the document. |
| **Summary Date:** | **23/08/2024** |
| **Completed by:** | **Julian Kenshole** |

**Staff Acceptable Use Policy**

Bishop Hogarth Catholic Education Trust (Trust) networked resources, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the Trust. If you make a comment about Trust or any school or college within the Trust you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the Trust or any school or college within the Trust into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user’s access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

[Amended]This policy should be read in conjunction with the school’s Data Protection Policy, Information Security, On-line Safety, Social Media and Email Policy.

# CONDITIONS OF USE

**Personal Responsibility**

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network toa member of the senior leadership team*.*

**Acceptable Use**

Users are expected to utilise the network systems in a responsible manner. All computer systems and networks including personal devices connected to the Trust systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with.

|  |  |
| --- | --- |
| 1 | I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or cause needless anxiety to any other person or bring Trust or any school or college within Trust into disrepute. |
| 2 | I will use appropriate language – I will remember that I am a representative of Trust on a global public system. I am aware that illegal activities of any kind are strictly forbidden. |
| 3 | I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group. |
| 4 | I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored. |
| 5 [Amended] | I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21).  I will not reveal any of my personal information to students.  I will not communicate with pupils or parents over personal social media accounts. Accept ‘friend’ or ‘follow’ requests from any pupils or parents over personal social media accounts. |
| 6 | I will not trespass into other users’ files or folders. I am aware that staff accessing students work must be given permission before this can take place. |
| 7 | I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself. Likewise, I will not share those of other users. |
| 8 | I will ensure that if I think someone has learned my password then I will change it immediately and/or contact a member of the senior leadership team. |
| 9 | I will ensure that I log off after my network session has finished or will lock the computer to make it secure until my return. |
| 10 | If I find an unattended device logged on under other users username I will **not** continue using the device – I will log it off immediately. |
| 11 [Amended] | I will not use personal digital devices or camera phones for creating or transferring images of children and young people without the express permission from the senior leadership team. |
| 12 [Amended] | I am aware that e-mail is not guaranteed to be private. I am aware that messages relating to or in support of illegal activities will be reported to the authorities. I am aware that anonymous messages are not permitted. I will ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.  I am aware that all emails are backed up and that my emails in the backup may be searched if an investigation is required with or without my knowledge. I understand that my email account and other online/offline storage files can be searched if an investigation is required with or without my knowledge. |
| 13 | I will not use the network in any way that would disrupt use of the network by others. |
| 14 | I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to a member of the senior leadership team. |
| 15 | If I suspect that my computer has a virus, I must report it to a member of the ICT staff immediately. |
| 16 | I will not use “USB drives”, portable hard-drives, “floppy disks” or personal laptops any other device on the network (wired or wireless) on the network without having them “approved” by a member of the senior leadership team or Trust ICT Department. |
| 17 | I will not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils.  I am responsible for rejecting any links to such material which may appear inadvertently during research.  If I encounter any material which could be regarded as offensive, I will leave that website or service immediately and not make any copy of that material. I am aware that if I encounter any difficulty in leaving a website or service, I must inform the ICT support staff immediately. |
| 18 | I will not download/install any software, system utilities or resources from the Internet or digital device. |
| 19 | I will set up a secure pin code on my phone or similar connected device that is connected to the email system.  I will also notify Trust ICT Department immediately if a phone or similar connected device which is connected to the email system is lost or stolen. This will give the opportunity to disable your email access from such device |
| 21 | I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way. |
| 22 [Amended] | I will follow the Trust’s Data Protection Policy and support and promote the Trusts e-safety and Information Security policies and help students be safe and responsible in their use of the Internet and related technologies. |
| 23 | I will not send or publish material that violates the Data Protection Act or breaching the security this act requires for personal data. |
| 24 | I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting. |
| 25 | I will not attempt to harm or destroy any equipment or data of another user or network connected to Trust ICT Network. |
| 26 | I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. |
| 27 | I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured. |
| 28 | I will not plug non-school equipment into an electric socket at Trust or any school or college within Trust unless it has been PAT tested at school. |
| 29 | If I transport Trust / School / College equipment between home and Trust / School / College or another destination I will not leave the equipment unattended. |
| 30 [New] | I will participate in any relevant training offered to me, including Data Protection, cyber-security and online safety. |
| 31 | I understand that I must follow agreed protocols when using any ICT resources within Trust or any school or college within Trust |
| 32 [Amended] | At any time and without prior notice, Trust management reserves the right to examine my network activity, e-mail, personal file directories, and other information stored on Trust network and equipment. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Trust information systems. Permission to examine such information will only be granted by the Chief Executive Officer. |

**Additional guidelines**

* Staff must comply with the acceptable use policy of any other networks that they access.This includes any external system that Trust or any school or college within Trust is partnered with

# SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The Trust or any school or college within Trust will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

# NETWORK SECURITY

Users are expected to inform a member of the senior leadership team or Trust IT Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on Trust network will be regularly checked by Trust IT Manager by request of the senior leadership team. Users identified as a security risk will be denied access to the network. Users who want to have their smartphone or internet connected device used for remote access or email should first be authorised to have this feature enabled by Trust IT Manager or a member of the Senior Leadership Team. Any connected smartphone or tablet must have a secure pin number set in order to protect the email / remote access. Lost / Stolen devices should be immediately reported to Trust IT Manager or a member of the Senior Leadership Team

# MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students’ work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

**Social Media & Messaging**

All users should be aware of the risks associated through using Social Media & Messaging in their professional role. Becoming friends or following students on social media platforms is not acceptable with the only exception being where a member of staff has children within Trust or any school or college within Trust. Any use of personal social media that brings Trust or any school or college within Trust into disrepute will result in disciplinary action. Users should not use any form of internet messaging services within their role apart from those that are approved by Trust. **Staff and Trust schools will not create social media accounts without first seeking the authority of CEO /DCEO.**

**Pupil Acceptable Use Agreements**

An acceptable use agreement for older pupils (Key Stage 3-5) is attached at **Appendix 1.**

An Acceptable use agreement for younger pupils is attached at **Appendix 2**

Appendix 1

**Student Acceptable Use Agreement**

Bishop Hogarth Catholic Education Trustunderstands the benefits technology can have on enhancing the curriculum and pupils’ learning; however, we must ensure that pupils respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of pupils when using technology, whether this is on personal or school devices and on or off the school premises.

All students must follow the conditions described in this Agreement. Breaking these conditions may lead to:

* Withdrawal of the student’s access,
* Close monitoring of the students’ network activity,
* Investigation of the students’ past network activity,
* In some cases, criminal prosecution.

It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Agreement. Students must also accept personal responsibility for reporting any misuse of the network.

**Acceptable Use**

Students are expected to use the network systems in a responsible manner. All use must be consistent with the following list of expectations:

|  |  |
| --- | --- |
| 1 | I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute. |
| 2 | I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden. |
| 3 | I will not use language that could stir up hatred against any ethnic, religious or other minority group. |
| 4 | I realise that files held on the school network will be regularly checked by IT staff or other members of staff. |
| 5 | I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network. |
| 6 | I will not trespass into other users’ files or folders. |
| 7 | I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people’s username and password. |
| 8 | I will ensure that if I think someone has learned my password then I will change it immediately and/or contact a member of the IT Team*.* |
| 9 | I will ensure that I log off after my network session has finished. |
| 10 | If I find an unattended device logged on under other users username I will **not**  continuing using the device – I will log it off immediately. |
| 11 | I understand that I am will not be allowed access to unsupervised and/or nauthorized chat rooms and should not attempt to gain access to them. |
| 12 | I am aware that e-mail is not guaranteed to be private. Messages supporting of illegal activities will be reported to the authorities. Anonymous / unnamed messages are not permitted. |
| 13 | I will not use the network in any way that would disrupt use of the network by others. |
| 14 | I will report any accidental access to other people’s information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to a member of staff. |
| 15 | I will not introduce “USB drives” or other portable devices into the network without having them checked for viruses. |
| 16 | If I suspect that my computer has a virus, I must report it to a member of the ICT staff immediately. |
| 17 | I will not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils.  I am responsible for rejecting any links to such material which may appear inadvertently during research.  If I encounter any material which could be regarded as offensive I will leave that website or service immediately and not make any copy of that material. I am aware that if I encounter any difficulty in leaving a website or service, I must inform a member of staff immediately. |
| 18  [Amended] | I will think about what I post about the school on social media and make sure I do not post anything that could be harmful to any member of the school community.  I will not:  · Try to speak to any member of staff on social media.  · Accept or send ‘friend’ or ‘follow’ requests from members of staff on social media.  · Send any abusive, threatening or otherwise inappropriate messages on social media.  · Bully anyone through social media. |
| 19 | I will not download and/or install any software, system utilities or resources from the Internet. |
| 20 | I realise that students under reasonable suspicion of misuse in terms of time, activity or content may have their usage closely monitored or have their past use investigated. |
| 21 | I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting. |
| 22 | I will not attempt to harm or destroy any equipment or data of another user or network connected to Trust / school ICT Network. |
| 23 | I understand that unapproved system utilities and executable files are not allowed in my work areas or attached to e-mails. |
| 24 | I agree to comply with the acceptable use policy of any other networks that I access. |

Appendix 2

**Pupil Acceptable Use Agreement**

We know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have made this agreement to help you understand how to be safe when you are using technology. Please read this carefully so that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.

A close up of a screen

Description automatically generatedA screen shot of a computer

Description automatically generated

A picture containing clock

Description automatically generated

**I will:**

* A picture containing drawing

  Description automatically generatedOnly use technology, such as a computer, when a teacher has given me permission.
* Only use technology for the reason I have been asked to use it.
* Only use the internet when a teacher has given me permission.
* Ask for help when I have a problem using the technology.
* Look after the device and try not to damage it.
* Tell the teacher if my device is not working or damaged.
* Tell the teacher if I think someone else is not using technology safely or correctly.
* Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

**I will not:**

A picture containing drawing

Description automatically generated

* Tell another pupil my username and password.
* Share personal information, such as my age and where I live, about myself or my friends online.
* Access social media, such as Facebook and WhatsApp.
* Speak to strangers on the internet.
* Take photos of myself or my friends using a school device.
* [New] Say unkind things via email or social media.

|  |  |
| --- | --- |
|  |  |