Bryntirion Comprehensive School - ICT Acceptable Use Policy (Pupils)

Contents

Scope of this policy

1 Introduction

1.1 Bryntirion Comprehensive School is committed to protecting its pupils, from illegal or damaging use of technology by individuals, either knowingly or unknowingly.

1.2 As users of the School's IT services pupils have a right to use its computing services; that right places responsibilities on these users which are outlined below. Misuse of the computing facilities in a way that constitutes a breach or disregard of the following policy may also be in breach of other School policies.

1.3 Ignorance of this policy and the responsibilities it places on users is not an excuse in any situation where it is assessed there has been a breach of the policy and its requirements.

1.4 Pupils are NOT permitted to connect their own IT equipment to the School's network and the services available therein.

1.5 Pupils are directed to this policy during their induction and are required to acknowledge their agreed adherence to and compliance with the policy when they first log on to the network.

1.6 A copy of this policy is available to parents on request and on the school website and the School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

2 Purpose

2.1 The purpose of this policy is to:

2.1.1 outline the acceptable and unacceptable use of computer equipment or "on-line services" owned by the School, and acceptable or unacceptable general behaviour in ICT areas;

2.1.2 educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

2.1.3 safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

2.1.3.1 exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

2.1.3.2 the sharing of personal data, including images;

2.1.3.3 inappropriate online contact or conduct; and

2.1.3.4 cyberbullying and other forms of abuse;

2.1.4 help pupils take responsibility for their own safe use of technology (i.e. limiting the risks that children and young people are exposed to when using technology);

2.1.5 ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology.

2.2 These rules are in place to protect pupils and the School. Inappropriate use exposes the School and its Academic Partners to risks including virus attacks, compromise of network systems and services, and legal issues.

3 Scope

3.1 This policy applies to all pupils of Bryntirion Comprehensive School.

3.2 The School will take a wide and purposive 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 including:

3.2.1 the internet

3.2.2 email

3.2.3 mobile phones and smartphones

3.2.4 desktops, laptops, netbooks, tablets / phablets

3.2.5 personal music players

3.2.6 devices with the capability for recording and / or storing still or moving images

3.2.7 social networking, micro blogging and other interactive web sites

3.2.8 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards

3.2.9 webcams, video hosting sites (such as YouTube)

3.2.10 gaming sites

3.2.11 Virtual Learning Environments

3.2.12 SMART boards

3.2.13 other photographic or electronic equipment e.g. GoPro devices and other wearable technology.

3.3 This policy applies to the use of technology on School premises.

3.4 This policy also applies to the use of technology off school premises if the use involves pupils or any member of the School community or where the culture or reputation of the School or member of staff are put at risk.

4 Safe use of technology

4.1 We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

4.2 The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

4.3 Pupils may find the following resources helpful in keeping themselves safe online:

http://www.thinkuknow.co.uk

http://www.childnet.com

http://www.childline.org.uk/Pages/Home.aspx

5 Procedures

5.1 Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils he / she should talk to a teacher about it as soon as possible.

5.2 Any misuse of technology by pupils will be dealt with under the School's Behaviour and Discipline in School policy.

5.3 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anit-Bullying policy. If a pupil thinks that he / she might have been bullied or that another person is being bullied, he / she should talk to a teacher about it as soon as possible. See the School'sAnti-Bullying policy for further information about cyberbullying and e-safety, including useful resources.

5.4 In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's Child Protection and Safeguarding policy). If a pupil is worried about something that he / she has seen on the internet, or on any electronic device, including on another person's electronic device, he / she must tell a teacher about it as soon as possible.

5.5 In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

5.6 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead who will record the matter centrally.

6 Unacceptable Usage

6.1 The School provides internet access and an email system (through O365) to pupils to support their academic progress and development.

6.2 Unacceptable use of School technology and network resources may be summarised as, but not restricted to:

6.2.1 Actions which cause physical damage to any ICT hardware, including peripherals (e.g., mouse, cables, wiring, printers);

6.2.2 Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate;

6.2.3 Viewing, retrieving, downloading or sharing any offensive material which may include content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity;

6.2.4 Threatening, intimidating or harassing staff, pupils or others;

6.2.5 Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;

6.2.6 Defamation;

6.2.7 Unsolicited advertising often referred to as "spamming";

6.2.8 Sending emails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address;

6.2.9 Not adhering to the acceptable data storage levels set by the ICT Network Manager

6.2.10 Attempts to break into or damage computer systems or data held thereon;

6.2.11 Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware;

6.2.12 Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;

6.2.13 Using the School network for unauthenticated access;

6.2.14 Any other conduct which may discredit or harm the School, its staff, community or the ICT Facilities;

6.2.15 Using the ICT facilities for gambling;

6.2.16 Using the ICT facilities for carrying out any illegal trading activity.

6.3 This policy sets out the following rules and principles with which pupils must comply:

6.3.1 Authorisation - access and security

6.3.2 Use of the internet and email

6.3.3 Use of mobile electronic devices and

6.3.4 Photographs and images.

These principles and rules apply to all use of technology.

6.4 Anyone who mistakenly accesses inappropriate material should notify ICT Support.

6.5 The School may inform the police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

7 Sanctions

7.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the School may apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour and Discipline in School policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures and withdrawal of the right to access the School's internet and email facilities. Any action taken will depend on the seriousness of the offence.

7.2 Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy and the School's policy on the searching and confiscation of electronic devices contained in the Anti-Bullying Policy.

Key Principles and Rules

8 Data Storage and Backups

Data on school servers (pupils MyWork folder)

All data stored on the school servers is regularly backed up. The school operates a rolling monthly backup cycle i.e. data should be retrievable from a month prior to the current date. If data is accidently deleted from the pupils local network account then the pupil should contact the ICT Network Manager to arrange a data restore.

Data on O365 accounts

Data stored in the pupils O365 account (i.e. Onedrive or Outlook email) is not backed up by the school. If data is deleted it will reside in pupils O365 Recycle Bin for a maximum 93 days before being removed, unless the total size of the recycle bin exceeds 10% of total Onedrive storage, whereupon the duration of storage is reduced. Once this happens it **CANNOT BE RESTORED**! For this reason all school coursework/controlled assessment/NEA **MUST** be saved to the pupils local network account (the MyWork folder).

If a pupil leaves the school, then access to their O365 account is removed immediately. The ICT Network Manager can access their files for a further 30 days. After this time Microsoft deletes all files for the pupil account – the pupil data is then irretrievable.

9 Authorisation - access and security

9.1 In order to use the School's ICT Facilities pupils must first be properly registered to use such services. Registration to use School services implies and is conditional upon acceptance of this Acceptable Use Policy.

9.2 The registration procedure grants authorisation to use the core ICT Facilities of the School. Following registration, a username and password will be allocated to each pupil.

9.3 Any attempt to access or use any user account or email address, for which the pupil is not authorised, is prohibited.

9.4 Pupils may not use, or attempt to use, ICT resources allocated to another person, except when explicitly authorised.

9.5 Pupils must take all reasonable precautions to protect the School's resources (including the ICT Facilities and the School's information and data), their username and passwords.

9.6 Purpose of Use

9.6.1 ICT facilities are provided primarily to facilitate a person's work as a pupil. Use for other purposes, such as personal email or recreational use of the Internet, is only permitted during the permitted times specified by the School and is a privilege, which can be withdrawn at any time and without notice. Any such use must not interfere with the pupil's studies or any other person's use of computer systems and must not, in any way, bring the School into disrepute.

9.6.2 School email addresses and associated School email systems must be used for all official School business. All pupils must regularly read their School email and delete unwanted or unnecessary emails at regular intervals.

9.7 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. Pupils must not try to bypass this filter.

9.8 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If a pupil thinks or suspects that an attachment, or other downloadable material, might contain a virus, he / she must speak to a member of ICT Support staff before opening the attachment or downloading the material. Pupils must not disable or uninstall anti-virus software on the School's computers.

9.9 Privacy and Monitoring

9.9.1 All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. Pupils are personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person.

9.9.2 Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

9.9.3 For the protection of all pupils, their use of email and of the internet when accessed via the School network will be monitored by the School. Pupils should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system.

Pupils should not assume that files stored on servers or storage media are always private – the ICT Network Manager has access to all data stored on the school servers and with school O365 accounts.

9.9.4 Pupils must not interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly pupils must not make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

10 Use of the internet, email and O365 accounts

10.1 The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

10.2 Use of the internet

10.2.1 Pupils must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. Pupils must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Pupils must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

10.2.2 Pupils must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

10.2.3 Pupils must not bring the School into disrepute through their use of the internet.

10.2.4 Copyright Compliance

10.2.4.1 All pupils must abide by laws relating to the use and protection of copyright.

10.2.4.2 Pupils must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose e.g. research then copyright permission must be obtained and documented before such material is used.

10.2.4.3 Pupils are reminded that the School treats plagiarism very seriously and will investigate any allegation i.e. the intentional use of other people's material without attribution.

10.3 Use of email & O365

10.3.1 Pupils must use their School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

10.3.2 Email/O365 should be treated in the same way as any other form of written communication. Pupils should not include or ask to receive anything in an email/O365 which is not appropriate to be published generally or which they believe the School or their parents would consider to be inappropriate. Remember that emails/O365 content could be forwarded to or seen by someone they did not intend.

10.3.3 Pupils must not send or search for any email message/ O365 content which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If they are unsure about the content of a message, they must speak to a member of staff. If they come across such material they must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

10.3.4 Trivial messages and jokes should not be sent or forwarded through the School's email system or O365 shared areas. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the School's network to suffer delays and / or damage.

10.3.5 Pupils must not read anyone else's emails without their consent.

11 Use of mobile electronic devices

11.1 "Mobile electronic devices" includes but is not limited to mobile 'phones, smartphones, tablets, laptops and MP3 players.

11.2 Pupils are not permitted at any time to connect devices with a network cable in any part of the School or to any other school Wi-Fi network.

11.3 Mobile phones and other mobile electronic devices must be switched off (and not just on silent mode) and kept in bags during School hours, including at break times and between lessons. Use of such devices is only permitted during School hours with the express permission of a member of staff.

11.4 Pupils must not communicate with a member of staff’s personal (as opposed to School) mobile phone except when this is expressly permitted by a member of staff (e.g. if staff member has no school mobile and communication is required for the normal running of School business). For example this may on occasion be necessary during an educational visit. Any such permitted communications should be brief and courteous.

11.5 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not they are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-Bullying policy and Behaviour and Discipline in School policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's Child Protection and Safeguarding policy and procedures).

11.6 Mobile electronic devices may be confiscated in appropriate circumstances. Pupils may also be prevented from bringing a mobile electronic device into the School temporarily or permanently.

11.7 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

12 Photographs and images

12.1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. Pupils may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.

12.2 Pupils must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

12.3 The posting of images which in the reasonable opinion of the School is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

13. Sexting

'Sexting' means the taking and sending or posting of images or videos of a sexual or indecent nature, usually through mobile picture messages or webcams over the internet.

Sexting is strictly prohibited, whether or not the pupil is in the care of the School at the time the image is recorded and / or shared.

Sexting may also be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.

Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Child Protection and Safeguarding policy and procedures).

If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.

14 Responsibilities

14.1 This policy is the responsibility of the Headteacher.

14.2 The Headteacher is responsible for ensuring that issues around data protection and copyright compliance are monitored.

14.3 All School Managers are responsible for the implementation and monitoring of the policy.

14.4 Any suspected breach of this policy should be reported to a member of ICT

Support staff. A member of SLT will then take the appropriate action within the School's disciplinary framework; other members of the School ICT Support staff will also take action when infringements are detected in the course of their normal duties.

Appendix 1

1 ICT Services Acceptable Use Policy (AUP) Summary for Pupils

1.1 You must not:

1.1.1 Allow other people to use your account.

1.1.2 Download or access illegal software onto a workstation.

1.1.3 Download or copy any software packages from the School network onto portable media, etc.

1.1.4 Upload your own personal software packages onto a School workstation.

1.1.5 Access offensive or abusive material.

1.1.6 Send or receive offensive, abusive or inappropriate e-mails.

1.1.7 Access "inappropriate" websites - some Internet pages are illegal and may be subject to criminal proceedings.

1.1.8 Interfere with other users' work.

1.1.9 Photograph or record members of staff or pupils without their permission, using devices such as mobile phones, cameras or digital recorders.

1.1.10 Use software designed to unblock sites.

1.1.11 Use online gambling sites.

1.1.12 Use peer-to-peer and related applications anywhere on school premises. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus and KaZaA.

1.1.13 Abuse equipment.

1.1.14 Make offensive or inappropriate comments including bringing the School’s name and reputation into disrepute on any forum/platform, such as social media sites (whether using a school device or not) where a connection between the user and Bryntirion Comprehensive School can reasonably be made.

1.2 Please remember, when in teaching and learning areas such as the Library, ICT Suites or classrooms:

1.2.1 Keep noise to a minimum to avoid disrupting others.

1.2.2 Copyright regulations apply to electronic sources - please check before you print out from online services.

1.2.3 Logout or lock your computer when leaving a computer, even for a short time.

1.2.4 Be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc) has been electrically tested, before using it on School premises.

1.3 Anyone found abusing the School policy on the use of computers may have their network rights removed, and may be subject to further disciplinary action.

1.4 School computers are provided primarily for School work. However, you may use the equipment for personal use providing:

1.4.1 You do not breach the Acceptable Use Policy.

1.4.2 You are not doing so for gambling purposes.

1.5 If you use the School equipment for personal use you should note the following:

1.5.1 Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.

1.5.2 If you are using communal ICT facilities (such as the library), you may be asked to log-off where the demand for the equipment is high.

1.5.3 This Acceptable Use Policy applies to both wired and wireless access and use of network on your own equipment or on School equipment.

1.5.4 In order to use the ICT Facilities of the School you must first be properly registered to use such services.

1.5.5 Registration to use School services implies, and is conditional upon acceptance of this Acceptable Use Policy as part of the School regulations, for which a signature or electronic acknowledgement of acceptance is required on joining the School.

1.5.6 The lack of a signature does not exempt an individual from any obligation under this policy.

1.5.7 The continuing use of the ICT Facilities will be deemed to be acceptance by the user of the terms of this policy.

1.6 The school reserves the right to remove access at any time.

I have read and understood the above and agree to use the school digital technology systems and my own devices within these guidelines.

Name:…..

Signed:...

Date:..................................