POLICY STATEMENT

Policy	Acceptable Use of I.T. Policy (Pupils)
OFSTED Standard No	
School Department	Teaching, Learning, Assessment and Tracking

Date Written	27th April 2017
Written by	The Athena Programme Ltd, reviewed V Ireland 2017
Approved by	G Johnson
Date of Approval	11/ 5/ 17
Next major review date	14th December 2017
Location and disseminations	A copy of the policy can be found, in the school admin office and on the school website.
The context of the policy and its relationship to other policies	This policy should be considered in conjunction with other written policies on behaviour, health and safety, medicines, school visits, child protection and safeguarding.
Forms, feedback and reporting	Some policies have specific reporting forms (these would be indicated within the policy). However, don't panic if you cannot locate the correct reporting or feedback form you will find, next to every policy on the web site that there is an online report form and rating form for any feedback that you may wish to give.

1. Policy Statement

Buckswood School aims to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. This policy and the guidelines within it aim to protect pupils and students from e-safety incidents and promote a safe e-learning environment.

The School's ICT and related systems are important and essential assets which need to be appropriately protected. The School is concerned with establishing a framework of acceptable usage and controls, including pupil/student responsibilities, in order to safeguard our ICT hardware, systems, infrastructure and data from:

- unauthorised access
- accidental or intentional damage

- interruptions to availability of services
- use for illegal purposes

At Buckswood we believe that pupils and students should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

The aims of this policy are to:

- encourage pupils and students to make good use of educational opportunities presented by access to the Internet and electronic communication
- to safeguard and promote the welfare of pupils by preventing "cyberbullying" and other forms of abuse
- minimise the risk of harm to the assets and reputation of the School
- help pupils take responsibility for their own e-safety
- ensure that pupils use technology safely and securely

This policy applies to the use of technology on School premises and also any use, whether on or off School premises, which affects the welfare of other pupils or where the culture or reputation of the School are put at risk.

2. Procedures

Pupils/students are responsible for their actions, conduct and behaviour online in the same way that they are responsible at all other times. Use of technology should be safe, responsible and legal.

Pupils/students must not use their own or the School's or any other technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy. If you think that you might have been bullied or if you think another person is being bullied, talk to a member of staff about it as soon as possible.

If there is a suggestion that a pupil or student is at risk of abuse or significant harm, the matter will be dealt with under the School's Child Protection Safeguarding Procedures. If you are worried about something that you have seen on the Internet or on social media, talk to a member of staff about it as soon as possible.

Examples of acceptable use are:

- Using web browsers to obtain information from the Internet
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the school's network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school's network to access outside resources that conform to this "Acceptable Use Policy".
- Using the network and Internet in a manner, which respects the rights and property of

others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the school's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a teacher or supervising adult of the occurrence immediately.
- Logging out or locking computers when they are left unattended
- Recognise that electronic communications sent through or stored on the school's network will be treated as school related and may be monitored or examined by the Principal or her/his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes
- Reporting any damage to or loss of computer hardware immediately
- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems
- Reporting any inappropriate behaviour and online bullying to the safeguarding Coordinator
- Take reasonable care that there is no damage or loss of any equipment on loan from school

Expulsion is the likely consequence for any pupil/student found to be responsible for material on his or her own or another website or social medium or any other electronic material that would be a serious breach of School rules in any other context.

Any misuse of the Internet will be dealt with under the behaviour and discipline policies of the School. Examples of misuse are set out in the Appendix 1. Any misuse should be reported to a member of staff as soon as possible.

3. Sanctions

Where a pupil/student breaches any of the School's protocols, the Principal will apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include increased monitoring procedures, detention or the withdrawal of privileges.

Unacceptable use of electronic equipment could lead to confiscation and other disciplinary sanctions in accordance with the rules set out in this policy, the student handbook and the behaviour and discipline policy.

4. Electronic Mail (email) and the Internet

These communications facilities are provided as essential teaching and learning tools and we encourage all our pupils/students to use these tools effectively and appropriately in support of their work.

When using e-mail, you must ensure that you do not create, access, or pass on material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, bullying, incites or depicts violence or terrorist acts or is otherwise inappropriate or represents values which are contrary to Buckswood School's Guidelines. School e-mail is routinely monitored fur such activity by the IT Services Department.

All incoming and outgoing electronic data will be monitored for inappropriate content and threats such as computer viruses and other potentially harmful programs.

The use of e-mail services, other than that provided by the school, is not supported from within the school.

The Internet is provided as a resource in support of your studies. All Internet activity is monitored and logged. Attempts to access or download material from obscene, unlawful, violent, abusive or similar sites deemed inappropriate for a School environment will be punishable under the terms of the student handbook l and the behaviour and discipline policies.

5. Security and Confidentiality

It is essential that our computer systems and data are secure. To help achieve this we require pupils/students to be aware of the need to protect IT equipment and data from actions and misuse which could affect the confidentiality, integrity and availability of our systems and data.

Security of IT applies to the use of the IT hardware and facilities which are either supplied by Buckswood School or in the use of personal equipment authorised for use on the systems (both on and off the premises).

USB Dongles

Accessing the Internet on a school laptop using a USB dongle presents a major threat to the school's network security. Please ensure these are checked for viruses before inserting them into school equipment.

Passwords

At the core of all data security is the passwords you may require to access the network and related systems. If you have been issued with a username/password to access resources on the network:

- The password should be changed at the first opportunity (if the system permits)
- Passwords must be a minimum of 8 characters and should include letters and numbers
- Personal passwords should never be shared with friends
- Pupils have the responsibility to safeguard their passwords and change them regularly to avoid breaches in security and immediately if they suspect they may have been compromised.

Security of Hardware

Pupils are welcome to use their own laptops and mobile devices in accordance with the one device per student online arrangement and in regards to the adherence to the no mobile phones rule. Please contact the IT Services for further information.

All activity on the school's computing facilities is monitored which will alert IT Services to any breaches of this policy.

Access to IT systems must only be made via your authorised user account and password. Accounts should never be left open whilst unattended and users must always log off when finished. This will then require a password to be entered before the computer can be used again and guard against unauthorised access.

At the end of the working day you must log out of your computer and shut down for security.

You must not use another person's account for any reason.

Any items of IT equipment are used at your own risk and the school accepts no liability for loss or damage as these items are your sole responsibility. Boarders are provided with a safe in their rooms for secure storage of personal items. Parents are advised to notify the school in the Starter Pack to log all relevant ID numbers of such equipment.

You must not attempt to move, re-configure, or alter the cabling on computer hardware or peripherals without the authority and assistance of an IT Technician.

To ensure compatibility with, and the security of, our systems, personal and other equipment which has not been purchased through the School Laptop Scheme or the IT Department may only be connected to computer systems or the network (wired or wireless) with the prior authority of the Information Systems Manager and inspection/configuration by an IT Technician. The equipment may be required to meet minimum standards before connection is undertaken.

To avoid potential conflicts or interference with school systems, software which has not been purchased through, or provided by, the IT Department may not be installed on School computer systems without the authority of the Information Systems Manager.

Safe use of IT
We want pupils/students to enjoy using IT and to become skilled users of online resources and media. We recognise that this is crucial for lifelong education and careers.

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

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

6. Social Media

Social media are powerful allies and appropriate use is encouraged. Inappropriate use of social media, by whatever means, will be dealt with severely, under the terms of the School's Anti-Bullying Policy and under the terms of this ICT policy.

Such misuse may include, although is not restricted to, impersonating another person online, Frape, malicious or defamatory posts or messages and any action which is designed to undermine or defame another member of the School community.

Posting any information that detracts from the School's reputation is not allowed and will results in sanctions.

7. Monitoring and Review

The policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments made to the relevant legislation and in doing so will consider any e-safety incidents that have occurred. As with other school policies it will be reviewed at least once a year.

Appendix 1

Examples of unacceptable use

- Use of the Internet for purposes that are illegal, unethical, harmful to the school, or non-productive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or taking photographs on school premises without permission and with consent of the parent or carer.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Relocating school information and communication equipment without prior permission
- Posting any information that detracts from the School's reputation is not allowed and will result in sanctions.
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers
- Doing harm to other people or their work.
- Do not install software on school computers unless authorised by the ICT Team.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarising and violation of copyright laws.
- Conversation in email using all upper-case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your

files.

- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work, or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number. Use the school's address instead, but not the school's phone number.
- Downloading material from the Internet without specific authorisation from the ICT manager.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity.