POLICY STATEMENT

Policy	Online safety policy
OFSTED Standard No	
School Department	Safeguarding

Date Written	13th April 2017
Written by	G Sutton
Approved by	SMT
Date of Approval	13th April 2017
Next major review date	August 2018
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.

Buckswood recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to regulate ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our Cyber Bullying and Behaviour Policies.

For more information on data protection see also data protection policy.

Roles and Responsibilities

The school online safety coordinator is Mr Foster

Principal and SMT

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety co-ordinator. Any complaint about staff misuse must be referred to the online safety coordinator at the school or, in the case of a serious complaint, to the Proprietor.

We will:

- Ensure access to induction and training in online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SMT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Management Team will receive monitoring reports from the ICT Manager.
- Ensure weekly print offs are taken of usage and results shared with the Principal. These results will be used to track patterns of inappropriate use.

Online safety coordinator:

- Leads E-safety meetings.
- Work in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments,
- Reports to SMT.
- Liaise with the nominated member of the Senior Management Team & Proprietor to provide an annual report on online safety.

ICT Manager / Technical Staff:

The ICT Manager is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal; online safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

Communicating School Policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during workshops where personal safety, responsibility, and/or development are being discussed.

Making use of ICT and the Internet in school

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Pupils may find these resources useful to help you keep safe online:

http://www.thinkuknow.co.uk/
http://www.childnet.com/
http://www.childline.org.uk/Pages/Home.aspx

Some of the benefits of using ICT and the Internet in schools are:

For pupils:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the *DSL.* Sites judged to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from IT Technician

For more information on data protection in school please refer to our **data protection policy**. More information on protecting personal data can be found in **section 11** of this policy.

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 IT Department.

School Email Accounts and Appropriate Use

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Staff should be aware of the following when using email in school

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school, from a parent or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class

- Excessive social emailing will be restricted

- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

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.

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.

Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. **For information on the school policy on children's photographs on the school website please refer to this acceptable use of IT Policy.**

Policy and Guidance of Safe Use of Children's Photographs and Work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers indicate that they agree to the terms of conditions, which includes the right of the school to use student images in promotional material. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- School policy on the storage and deletion of photographs.

Parents in signing the application form give consent and can opt out of this by writing to the school

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

Parental consent must be obtained. Consent will cover the use of images in:

- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects
- electronic and paper images will be stored securely
- names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Parents will be told at the beginning of an event if photos are permitted. Events recorded by family members of the students such as school plays or sports days must be used for personal use only. **These images may not be used on Social Media unless on the school's official accounts.**
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our **school child protection and safeguarding policy.**

Complaints of Misuse of Photographs or Video

Parents should follow the school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools **child protection and safeguarding** policy and **behaviour policy.**

Our pupils increasingly use electronic equipment on a daily basis to access the internet and share content and images via social networking sites such as facebook, twitter, MSN, tumblr, snapchat and instagram.

Unfortunately some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings.
Pupils may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. Serious incidents may be managed in line with our sexual exploitation policy or child protection procedures.

Many pupils own or have access to hand held devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community.

Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.

Safe and professional behaviour of staff online will be discussed at staff induction.

Personal Social Media

1. School staff WILL NOT invite, accept or communicate with parents and students through any personal social media.
2. If a Student attempts to communicate with a member of staff through any Social Media applications, this must be reported to the Designated Safeguarding Lead.
3. Members of School Staff should set personal social media accounts to the highest levels of privacy settings available.
4. Staff must not publish posts or comments which refer directly or indirectly to matters related to the school and members of its community and must consider the reputation of the school with any posts, in line with contractual duty of contractual obligations.
5. All communication between staff and students should be made through and official school email account or school phone. Staff should not use a personal email account or mobile to make contact unless given prior approval by SMT.

Professional Social Media

1. All communication and social media content MUST be for the promotion of the school and its students, and accounts must be approved by the PR office.

2. All personal details of members of staff MUST NOT be placed on social media.
3. Social media uploads must be in good taste- never negative to Buckswood, students, staff or other institutions.
4. Politics, sex and religion MUST NOT be discussed – in line with our internationalism.
5. Staff must not publish photographs of a child if a parent has opted out of photographic use. If a member of staff is unsure, contact pr@buckswood.co.uk
6. Professional Social Media accounts must be registered with an official school email address and the log-in information should be provided to pr@buckswood.co.uk
7. Any abusive or inappropriate comments regarding the school must be immediately removed and reported to pr@buckswood.co.uk

Student Social Media

1. Students should be aware that third parties such as the media, school and police could access and view their profile and personal information and that inappropriate material found by these third parties could damage the reputation of the school and the student and have a negative impact on future prospects.
2. Students MUST NOT attempt to make contact with a member of staff through social media, and if a member of STAFF attempts to make contact with them should report it to the DSL.
3. Students must not post any personal information about themselves or other members of Buckswood staff and student, imagery of the campus or illegal/ distasteful activity whilst in school uniform or within school hours. This could lead to suspension or expulsion.
4. Be aware of copyright and intellectual property rights. Before publishing content, ensure that they have permission of the owner. Infringement could lead to legal action.
5. The school logo, campus and any intellectual property can only be used on social media with the approval of the school.
6. Students must not publish content that can represent the school in a negative light, whether this is on a professional or personal social media profile.
7. The PR department and Social Media team will regularly review social media postings and any content they do not see as suitable MUST NOT be posted to any social media accounts and must be removed immediately.

Disobeying the guidelines above could lead in disciplinary action and may include suspension or expulsion.

Mobile Phones and Personal Device - for additional information on mobile phone usage by staff, please read the Code of Conduct

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- can make pupils and staff more vulnerable to cyberbullying
- can be used to access inappropriate internet material
- can be a distraction in the classroom
- are valuable items that could be stolen, damaged, or lost
- can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

- The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy.**
- A member of staff can confiscate mobile phones, and a member of the senior management team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile phones must be switched off during school lessons or any other formal school activities.
- Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

Mobile Phone or Personal Device Misuse

Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Staff

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.

- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff code of conduct

Cyberbullying - for full information please read the cyber bullying policy

The school, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour and anti-bullying / cyber bullying policies.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting Personal Data

Buckswood believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's data protection policy.**

SUMMARY

ACCEPTABLE USE: CODE OF CONDUCT (for Students):

IT/ONLINE SAFETY

At Buckswood we believe that pupils and students should be trusted to use digital technologies in a principled and productive way.

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.

1. 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 Code".
- 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.

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 without 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.