King William's College & The Buchan School

E-Safety Policy

King William's College & The Buchan School E-Safety Policy

1. Introduction

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

1.2 However, the use of these new technologies can put young people at risk within and outside the school. In addition the school uses images to market the school and to celebrate student's achievements and increasing numbers of parents wish to record their child's success in sport, drama and music, CCTV is used to protect the school, and students must have access to the internet for academic and leisure purposes. It is therefore important to have a robust and effective policy in place at King William's College & The Buchan School.

1.3 King William's College & The Buchan School are successful boarding and day schools. Proportionate measures are in place to control the use of electronic communications in order to detect abuse, bullying or unsafe practice by or towards any student. This e-safety policy should help to ensure safe and appropriate use.

1.4 Some of the dangers students may face include:

- Access to illegal, harmful or inappropriate images or other content

- Unauthorised access to / loss of / sharing of personal information

- The risk of being subject to grooming by those with whom they make contact on the internet.

- The sharing / distribution of personal images without an individual's consent or knowledge

- Inappropriate communication / contact with others, including strangers

- Cyber-bullying

- Access to unsuitable video / internet games

- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement

- Illegal downloading of music or video files

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

- Online gambling.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience (and staff) to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1.5   The school has provided the necessary safeguards to help ensure that everything that could reasonably be expected of us to manage and reduce these risks, is in place. This e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2.   Schedule for Development/Monitoring/Review

2.1   The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

2.2   The school will monitor the impact of the policy using:

- Logs of reported incidents

- Internal monitoring data for network activity

3.   Scope of this Policy

3.1   This policy applies to all members of the school community (including all staff, students, volunteers, parents and visitors) who have access to and are users of school ICT systems, both in and out of school. This policy includes the use of ICT, mobile phones and other electronic devices, and CCTV.

3.2   The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

4.   Roles and Responsibilities

4.1   The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

- Governors are responsible for the approval of the E-Safety Policy.

Principal and Leadership Team

- The Principal and the Leadership Team are responsible for the implementation and monitoring of this E-Safety policy as well as supporting those in school who carry out the internal e-safety monitoring role.

- The Principal is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated.

- The Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

- The Principal and another members of the Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

4.2   E-Safety Co-ordinator (currently the Deputy Head Pastoral at KWC and Alan MacNair at The Buchan)

- leads the e-safety committee

- liaises with the Designated Person for Child Protection

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place, and have signed to confirm that they understand

- organises training and advice for staff

- liaises with school ICT technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

- reports regularly to the Leadership Team.

4.3   IT Technical Staff

With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our students to understand why they need to behave responsibly if they are to protect themselves. Our technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage to the Deputy Head Pastoral.

The IT Technical Staff are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack. All equipment should be protected both physically and by software measures.

- that Common Room and Staff have all signed the Employee Acceptable Use Policy (Appendix A) and that students and their parents have signed the Students Acceptable Use Policy (Appendix B).

- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.

- the school's filtering policy, (Appendix C) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the network / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator/Deputy Head Pastoral for investigation.

- that monitoring software is implemented and updated as agreed in this and other school policies.

4.4 Common Room and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

- they have read, understood and signed the school Employee Acceptable Use Policy (Appendix A). Flouting this policy is regarded as a disciplinary offence.

- they report any suspected misuse or problem to the E-Safety Co-ordinator/Deputy Head Pastoral for investigation.

- digital communications with students should be on a professional level and only carried out using official school systems.

- e-safety issues are embedded in all aspects of the curriculum and other school activities.

- students understand and follow the school e-safety and acceptable use policy.

- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- they monitor ICT activity in lessons and boarding houses.

- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and must make sure that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.5 Designated Person for Child Protection

We recognise that internet safety is a child protection and general safeguarding issue. Our Designated Person has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. They works closely with the Isle of Man Safeguarding Children's Board and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of King William's College & The Buchan School. All of the staff with pastoral responsibilities receive training in e-safety issues. The school's comprehensive PSHE programme on e-safety is the Designated Person's responsibility, in conjunction with the Head of PSHE. They will ensure that all year groups in the school are educated as to the risks and the reasons why they need to behave responsibly online. It is their responsibility to handle allegations of misuse of the internet and should be aware of the potential for serious child protection issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming

- cyber-bullying

4.6 Students

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy (Appendix B), which they and their parents will be expected to sign before being given access to school systems.

- must act reasonably and consider others e.g. do not download large files during peak times as this will affect other users.

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

- are not allowed to participate in online gambling in any form.

4.7 Parents and Guardians

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact parents if we have any concerns about their children, and hope that parents will feel able to share any concerns with us. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. We are willing to provide discussion evenings for parents if necessary, either through a visiting specialist or by King William's College & The Buchan School staff, in order to advise about the potential hazards, and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

5. Policy Statements

5.1 Education of Students

5.1.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT and PHSE lessons and is regularly revisited –this covers both the use of ICT and new technologies in school and outside school.

- Key e-safety messages are reinforced as part of a planned programme of assemblies, tutorials and pastoral activities.

- Students are taught to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of information. They are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Students need to understand the need for the student AUP and will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

- Rules for use of ICT systems ("Student Acceptable Use Policy") should be read, acknowledged and signed by all students and their parents.

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

5.2   Common Room /Support Staff

5.2.1   It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

- Updates to the e-safety will be communicated to all staff and it is their responsibility to read and understand the current policy.

- EduCare online training is available for online safety and GDPR. This should be completed within the probation period for new teaching and support staff.

6. Technical Infrastructure

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- There will be regular reviews and audits of the safety and security of school ICT systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

- Any actual or potential e-safety incident should be reported to the Network Manager and E-Safety Co-ordinator.

- Both physical and non-physical (software based) security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

6.1   LAN

- All users will have clearly defined access rights to school ICT systems.

- Non IT Support Staff will not install programmes on school workstations / school portable devices.

- All users in the Senior School and Buchan Prep School will be provided with a username and password by the IT department who will keep an up to date record of users and their usernames. All users will be required to change their password at the start of every academic year. In the Buchan Pre-Prep School, group or class log-ons and passwords will be used, but teachers need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by students in this way should always be supervised and members of staff should never use a class log on for their own network access.

- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Head or other nominated senior leader who will be granted "Administrator" rights over all systems and these details (username/password) will be kept in a secure place (e.g. school safe).

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system will be in accordance with the relevant AUP.

- Departing staff, students and visitors will have their access terminated on the last day of their employment.

6.2 Internet / Web Filtering

Access to the internet via the school's network will be filtered according to the document "King William's College & The Buchan School web filtering policy".

The school maintains and supports the managed filtering service.

In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head (or other nominated senior leader).

- Any filtering issues should be reported immediately to the Network Manager.

- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Head of ICT, referring to ST if necessary. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

- Users will not be able to download executable files.

- The school infrastructure and individual workstations are protected by up to date anti-virus software, malware software and ransomware software, and by regular security updates.

- The school will maintain a record of all staff and students who are granted access to the school's electronic communications on the basis of educational need.

- All web activity is recorded and logs are retained for 1 month.

- Abuses are reported to pastoral staff.

6.3   School WiFi

- There is open access to the school WiFi for personal use (with a valid account and certification)

- This goes through the Web Filter so the same rules apply as for 4.2 above.

- We reserve the right to block any device.

6.4   CCTV

The use of CCTV can be affected by a number of Acts including the Data Protection Act, the Human Rights Act and the Regulation of Investigatory Powers Act (RIPA). King William's College & The Buchan School works to comply with these Acts.

6.4.1   Signage

- The purpose for which the system has been installed is stated on signage and is placed in prominent positions to inform the public that they are entering an area where their images are being recorded.

- The equipment is sited in such a way that it only monitors those spaces that are intended to be covered by the equipment.

- Operators (staff who operate and monitor CCTV) are aware of the purposes for which the scheme has been established.

- Operators are aware that they are only able to use the equipment in order to achieve the purposes for which it has been installed.

6.4.2   Use of CCTV

King William's College & The Buchan School will:

Consider if CCTV is the only viable option prior to installation.

Ensure that the Data Protection Notification (public register completed by data controllers detailing what processing of personal data is being carried out and sent to the Information Commissioner) covers the purposes for which the equipment is used; Review both the use of the CCTV system and the procedures to ensure compliance with the law.

- Not keep film/images for longer than necessary.

- Process images in a lawful manner.

- At the point of obtaining images the following will be provided:

- The name and address of the school

- The name and address of party acting on behalf of data controller, alerting public to who is processing the CCTV images.

- The purpose for which the images are intended to be used; and

- Any information which is necessary, having regard to the specific circumstances in which the images are, or are to be, processed to enable processing in respect of the individual to be fair.

- Establish and document the person(s) who are responsible for ensuring day-to-day compliance with the requirements of the Code of Practice.

- Make certain there are procedures for dealing with police enquiries, i.e. access under the DPA or removal of evidence under Police and Criminal Evidence Act.

King William's College & The Buchan School will not:

- Film areas that could amount to an infringement of personal privacy.

- Ignore subject access requests (an individual's written request to access information about themselves under the Data Protection Act). A person identifiable on CCTV images may be entitled to view the footage and may make a request to do so.

- Use CCTV footage for any other purpose other than what it was originally used for, e.g. prevention and detection of a crime.

- Use covert monitoring without seeking legal advice.

- Use Intrusive Surveillance at all.

- Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence.

- Disclose data to third parties, unless it is lawful to do so.

- Systematically monitor people by use of CCTV unless authorisation is sought under RIPA.

6.5   The school infrastructure and individual workstations are protected by an up to date anti-virus system.

7. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Support Team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

8. Use of Digital and Video Images

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes and the digital / video images must be deleted if no longer required.

- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance (and adhere to the current photo consent form) on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents will be obtained before photographs of students are published on the school website.

- Student's work can only be published with the permission of the student and parents.

8.2 The school provides a folder on the 'm' drive for storage of all photographs taken at school events. These photographs cannot be used without permission from the E Safety Co-ordinator or used for private purposes. Records are kept in the External Relations office (and iSAMS) of all students whose photographs cannot be used.

9. Data Protection

9.1 The School has data protection policies (Isle of Man and GDPR) for staff, students and parents. These can be found on the School website.

10. Communications

10.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following activities are not allowed for both staff and students:

- Use of mobile phones in lessons.

- Use of school email for personal emails.

- Taking photos or videos on mobile phones or other camera devices without prior permission.

- Storage of student mobile phone numbers on personal phones for longer than necessary.

10.2   When using communication technologies the school considers the following as good practice:

Email

- All students and staff will be provided with a school email address.

- The official school email service may be regarded as safe and secure.

- Users need to be aware that email communications may be monitored.

- Users must immediately report, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and students or parents must be professional in tone and content.

- Students must be taught about email safety issues, such as the risks attached to the use of personal details. They must also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Staff should only use School email accounts to communicate with students and other staff and external organisations if it involves school business.

- Email sent via the School's system should not be considered private and the School reserves the right to monitor email.

- Students should be reminded NOT to reveal any personal details of themselves or others in ANY communication, email or otherwise.

Social Networking / Social Media (There is a separate Social Media Policy for staff)

- We recognise that social networking and e-safety go hand-in-hand, so in addition to those separate policies, consider the following guidelines and precautions:

- Students should be taught about the use of social networking sites and the risks associated with revealing information.

- Students are advised through ICT lessons and PSHE never to give out personal details of any kind which may identify them and their location. Examples include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of family/friends, specific interests and clubs etc.

- Students are advised not to place personal photographs on any social networking site. They are advised to consider how public the information is and consider using private areas,

- The school maintains a very active social networking presence, using Facebook, Twitter, blogs, and more. These accounts are all centrally controlled by the External Relations department with careful password protection.

- Staff and students should be aware of the dangers of communicating via personal networking sites and should try to communicate through the official school social networking accounts.

- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.

- Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

- For responsible adults social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image once published.

- All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

School Website

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

- The School's website must not contain any personal information of staff or students.

- When information is placed on the School's website consideration must be given to intellectual property rights and copyright.

- The content of the School's website should be reviewed regularly to ensure that all material is appropriate for the intended audience.

- Publishing of any images of students can only take place with the permission of their parents and then must be decent and not reveal personal information.

Mobile Phones

- Mobile phones, iPods and other personal electronic devices should be switched off and stored securely during the school day. They may be used during lunch times and in boarding houses after school.

- Staff may confiscate personal equipment that is being used during the school day for the rest of the day. The equipment is usually stored in the Principal's office and students can sign to collect it from there.

- Sanctions may be imposed on students who use their electronic equipment without consideration for others.

- Houses use duty phones instead of personal phones for the day to day running of the house.

11. Unsuitable / Inappropriate Activities

11.1   We will not tolerate any illegal material, and will always report illegal activity to the police and/or the Isle of Man Safeguarding Children Board (SCB). If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our anti-bullying policy.

11.2   The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

- Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

    o   child sexual abuse images.

    o   promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation.

    o   adult material that potentially breaches the Obscene Publications Act in the UK.

    o   criminally racist material in UK.

    o   pornography.

    o   promotion of any kind of discrimination.

    o   promotion of racial or religious hatred.

    o   threatening behaviour, including promotion of physical violence or mental harm.

    o   any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

    o   online gambling.

11.3   Users shall not:

- Use school systems to run a private business

- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.

- Upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.

- Revealing or publicising confidential or proprietary information (eg financial/ personal information, databases, computer / network access codes and passwords).

- Create or propagate computer viruses or other harmful files.

- Carry out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.

- Participate in online gambling of any kind.

11.4 Users of mobile devices in School must ensure that appropriate anti-virus protection is enabled and up to date.

11.5 Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

<u>Students</u>

The following will be referred to the Police: Deliberately accessing or trying to access material that could be considered illegal including:

- child sexual abuse images

- adult material which potentially breaches the Obscene Publications Act

- criminally racist material

- other criminal conduct, activity or materials

The following will be subject to disciplinary action:

- Unauthorised use of mobile phone / digital camera / other handheld device.

- Unauthorised use of social networking / instant messaging / personal email.

- Unauthorised downloading or uploading of files.

- Allowing others to access school network by sharing username and passwords.

- Attempting to access or accessing the school network, using another student's account.

- Attempting to access or accessing the school network, using the account of a member of staff.

- Corrupting or destroying the data of other users.

- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.

- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.

- Using proxy sites or other means to subvert the school's filtering system.

- Deliberately accessing or trying to access offensive or pornographic material.

- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.

  <u>CR / Staff</u>

  The following will be referred to the Police:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).

- The following will be subject to disciplinary action:

- Allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.

- Careless use of personal data eg holding or transferring data in an insecure manner

- Deliberate actions to breach data protection or network security rules

- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software

- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature

- Actions which could compromise the staff member's professional standing

- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school

- Using proxy sites or other means to subvert the school's filtering system

- Deliberately accessing or trying to access offensive or pornographic material

- Breaching copyright or licensing regulations

  If members of staff suspect that misuse might have taken place it is essential that this is reported appropriately and promptly.

Related Policies

- Anti-Bullying Policy

- Behaviour Policy

- Web Filter Settings Policy

- Social Media Policy for Staff

- Data Protection Policy

- Safeguarding and Child Protection Policy

King William's College

Acceptable Use Policy

Students

This Acceptable Internet Use Policy replaces and supersedes all previous versions.

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that College systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

1. **General**

    1.1. I understand that the College regularly monitors use of the ICT systems, email and other digital communications of all its users for my protection.

    1.2. I will only use the College's computers for schoolwork, prep and as directed.

    1.3. I will act as I expect others to act towards me. In particular I will respect others' work and property, and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.

    1.4. I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language, and I appreciate that others may have different opinions.

    1.5. I will act responsibly in my use of Social Networking websites, and make sure that my posts do not bring the College into disrepute.

    1.6. I agree that my image or likeness can be used on the College website or in any promotional material published by the College or associated agencies, with permission of my parents via the photo permission form.

    1.7. Files brought in on removable media (such as flash drives etc.) may be deleted automatically (without warning) if they are found to contain viruses.

    1.8. I will not eat or drink near computer equipment.

2. **Cyberbullying** is the use of information and communication technologies, particularly mobile phones and the internet, to support deliberate, inappropriate behaviour by an individual or a group, that is intended to harm another individual or group. This may be on a single occasion or repeated over a period of time.

    2.1. I understand that the College considers cyberbullying a serious offence, both within and outside College. I will report any incident of cyberbullying to the Designated Person for Child Protection, which will be logged and followed up in accordance with the College's Anti-Bullying Policy.

3. **Internet**

    3.1. I will use the internet responsibly and will not visit websites I know to be banned by the College. I am also aware that during lessons I should only visit websites that are appropriate for my studies. If I am unsure if a site is safe I will ask a member of staff. The internet is NOT a secure means of transferring information.

    3.2. I will report any misuse of the internet immediately to a member of staff.

    3.3. I will not attempt to set-up or use any proxy by-pass software in order to by-pass the College internet filter. Any misuse could result in disciplinary action.

    3.4. I will not take information from the internet and pass it off as my own work **(plagiarism and copyright infringement.)**

    3.5. I will be responsible in my use of email and any other electronic communications. I will not include any material that is inappropriate or use offensive or threatening language in my emails or in any other communication on the internet. I understand that any email going out from the College will carry the College address and so represents the College. College email addresses will remain active for only one year after graduation.

3.6. I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.

3.7. I will not use the College ICT system for on-line gaming, on-line gambling, file sharing or video broadcasting, unless I have permission of a member of staff to do so.

4. E-Safety

4.1. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.

4.2. I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room, unless I take a trusted adult with me.

4.3. If I see anything I am unhappy with or I receive a message I do not like (both in and out of College), I will not respond to it but I will save it and talk to a teacher/trusted adult.

4.4. I am aware that some websites and social networks have age restrictions and I should respect this.

4.5. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk either when accessing the internet through the College network or through personal hardware (e.g. laptops and mobile phones).

4.6. I will not attempt to impersonate another person online e.g. post comments and access online accounts (Facebook, webmail) belonging to someone else.

5. Network.

5.1. I will keep my logins, IDs and passwords secret. I will not share them, nor will I try to use any other person's username and password. If I feel that password security has been compromised, I will report this to the IT Support Staff and change my password immediately.

5.2. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. Any suspicious emails should be reported to ICT support immediately.

5.3. I will not bring files into College (on removable media or online) without permission or upload inappropriate material to my workspace. I will immediately report any damage or faults involving equipment or software.

5.4. I will not attempt to gain unauthorised access to any part of the College's network that is not available from my personal logon, either via the network or the internet. I will not attempt to use or load programmes, files, tools or shortcuts to gain access to restricted parts of the network. I will immediately report any instance where I have inadvertently gained access to restricted areas to a member of staff.

5.5. I understand that this policy also applies when accessing the College's network or systems through my own hardware. For example, accessing the College's wireless network through a Wi-Fi enabled device. I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission from a member of staff.

STUDENT AUP (ACCEPTABLE USE POLICY)

Permission Form for Students

Please read this document carefully. If you violate these provisions, access to the Internet and School network will be denied and you may be subject to disciplinary action. If for any reason you think some has accessed your area, inform the ICT staff immediately.

Additional action may be taken by the College in line with existing policy regarding behaviour. For serious violations, suspension or exclusion may be imposed. Where appropriate, police may be involved or other legal action taken.

Please sign and return this permission form to the Head of Year.

Name of Student: _____ **Year Group:** _____

I agree to follow the College's Acceptable Use Policy.

Student's Signature: _____ **Date:** _____

Parent/Carer/House Parent

As the parent or legal carer of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter, or the child in my care, to access the College's ICT network and resources for educational purposes. I understand that while every reasonable precaution will be taken by the College to provide for online safety, the College cannot be held responsible if students access unsuitable websites.

Name: _____

Signature: _____ **Date:** _____

King William's College & The Buchan School

Acceptable Use Policy

Staff and Volunteers

The College reserves the right to amend this Acceptable Internet Use Policy, at any time, without notice. It is your responsibility to ensure that you remain current with such changes.

This Acceptable Internet Use Policy replaces and supersedes all previous versions.

Issue Date: 06/18

Review Date: 03/19

Next Review: 03/21

IT Manager: David Butterworth (Interim IT Director)

Designated Person for Child Protection: Stuart Corrie (Deputy Head Pastoral)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This policy is intended to ensure that:
- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All King William's College and The Buchan School ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible Use Agreement
I understand that I must use King William's College and The Buchan School ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.

1. **For my professional and personal safety:**
1.1   I understand that the College will monitor my use of ICT systems, email and other digital communications. Whilst the College respects the privacy of staff, where there is reason for concern, the College reserves the right to monitor and intercept e-mail communication.
1.2   I understand the rules set out in this agreement also apply to the use of the College ICT systems (e.g. laptops, email, Learning Platform etc.) out of the College.
1.3   I understand that the College ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the College. The use of school laptops for work out of school and at home is subject to all of the conditions of this policy, as if they were laptops permanently used in school. The need to use a laptop at home will be by agreement with your Line Manager, and periodic health checks of the device may be required by IT staff.
1.4   I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password. If I feel that password security has been compromised, I will report this to the IT support staff and immediately change my password.
1.5   I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person.
2. **I will be professional in my communications and actions when using school ICT systems:**
2.1   I will not access, copy, remove or otherwise alter any other user's files without their express permission.
2.2   I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Care must be taken with the overuse of capitalised words in email communication.
2.3   I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the College's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless College equipment is not available. If I use my own device, the digital/video image must be uploaded on to the College system at the earliest

opportunity and deleted from my personal device. Where these images are published (e.g. on the College website) it will not be possible to identify by name, or other personal information, those who are featured.

2.4 I will not use College devices or hardware for the extensive storage of personal photographs.

2.5 I am aware that communications may be subject to a Subject Access Request under Data Protection legislation, and as such I will ensure that I am careful not to make any comments which I would not wish to be disclosed.

2.6 I will only use chat and social networking sites in College in accordance with the College's e-safety policy, and not make any posting which may bring the College into disrepute.

2.7 I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.

2.8 I will not engage in any on-line activity that may compromise my professional responsibilities.

3. King William's College and The Buchan School have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

3.1 When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment. I will also follow any additional rules set by the College about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

3.2 The use of personal email on the College ICT systems is permitted but must be reasonable.

3.3 I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. Any suspicious emails should be reported to ICT support immediately.

3.4 I will ensure that my data is stored on the servers to be regularly backed up (rather than just the desktop), in accordance with relevant policies.

3.5 I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by legislation of Tynwald) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

3.6 I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.

3.7 I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is permitted by the IT Manager.

3.8 I will not disable or cause any damage to College equipment, or the equipment belonging to others.

3.9 I will only transport, hold, disclose or share personal information about myself or others as outlined in the Staff Data Protection Policy. Where personal data is transferred outside the secure College network, it must be encrypted.

3.10 I understand that the data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority. If I find that I have access to data not deemed necessary for my role, I will report this to the IT Manager.

3.11 I will immediately report any damage or faults involving equipment or software, however this may have happened.

4. When using the Internet in my professional capacity or for school sanctioned personal use:

4.1 I will ensure that I have permission to use the original work of others in my own work.

4.2 Where work is protected by copyright, I will not download or distribute copies (including music and videos). Please remember that all teaching material produced in the School environment is the intellectual property of King William's College and The Buchan School.

4.3 I understand that I am responsible for my actions in and out of the school.

4.4 I understand that this Acceptable Use Policy applies not only to my work and use of King William's College and The Buchan School ICT equipment in school, but also applies to my use

of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by the College.

4.5   I understand that if I fail to comply with this Acceptable Internet Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and, in the event of illegal activities, the involvement of the police.

5. ICT Equipment

5.1   Any equipment issued to staff remains the property of the College and must be returned upon request.

5.2   Upon termination of employment at King William's College and The Buchan School, all College equipment must be returned and access to College email will be reviewed.

I have read and understand the above and agree to use the King William's College and The Buchan School ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer name: …………………………………………………………

Signed: ………………………………………………………………………….

Date: …………………………………………………………………………..

PROFESSIONAL RESPONSIBILITIES
When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

➢ Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.

➢ Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.

➢ Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.

➢ Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.

➢ Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.

➢ Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.

➢ Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.

➢ Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

➢ Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

THE BUCHAN SCHOOL

STUDENT ACCEPTABLE USE POLICY FOR ICT

This policy was written so that children can benefit from using the School's ICT network in a safe way.

6. General

6.1. I understand that the School can look at what any child is doing on the computer.

6.2. I will only use the School's computers for schoolwork and prep.

6.3. I will treat other people as I would like to be treated. I will not open or change anyone else's files unless they say I can.

6.4. I will be polite when I talk to other people using a computer.

6.5. I will not bring digital files or digital technology into School without a teacher's permission.

6.5.1. Mobile phones and smart devices are not allowed in school and must be left in the school office during the school day.

7. **Cyberbullying** is when someone uses ICT to try and upset someone else.

7.1. The Buchan School takes cyberbullying very seriously. I will tell a teacher who I trust if I think that someone is being bullied using ICT.

7.2. I will not try and use ICT to harm anyone else.

7.3. I will not pretend to be another person online.

8. Internet

8.1. I will use the internet properly and will not go to websites I know I should not be on.

8.2. If I don't know if a website is ok to go on, I will ask a teacher.

8.3. I will not copy information on the internet and pretend it is my own work. This is called plagiarism.

8.4. I will only use my own school email address when emailing at school.

9. E-Safety

9.1. When I am online, I will not give out any personal information, including my full name, address or age.

9.2. I won't arrange to meet someone I have met on the internet

9.3. I will tell a teacher if I see something that worries me online.

9.4. I will only open email attachments from people I know, or who my teacher has approved.

9.5. I know that some websites and social networks have age restrictions and I should respect this

9.6. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe

10. Network.

10.1.   I will not try to use any other person's username and password.

10.2.   I will not download a file, unless a teacher has said I am allowed.

10.3.   I will tell a teacher straight away if something is not working on the computer.

APPENDIX D - Internet Filtering Policy (Provisional) System defined categories

Name	Description	Staff	Students (School Day)	Students (After Prep)
Adverts	All advertising is placed in this category.	Denied	Denied	Denied
Alcohol & Tobacco	Manufacturers and distributors of alcoholic drinks and tobacco products, as well as websites that promote the use of alcohol or tobacco.	Allow	Denied	Denied
Arts & Entertainment	Music, cinema, theatre, museums, art galleries are all included. Live entertainment venues and comedy clubs. Sites that allow the download of media are explicitly excluded -they are listed under 'Streaming media & media downloads'.	Allow	Denied	Allow
Auctions	Online auction sites, and any site that offers services to aid buying or selling via online auctions -'auction sniping' etc.	Denied	Denied	Denied
Automotive	Vehicle manufacturers, dealers and servicing are all covered by this category. Sites that allow traders or the general public to buy or sell vehicles. Clubs for specific manufacturers/models are applicable, as are discussion groups.	Allow	Allow	Allow
Business & Commercial	Businesses and commercial organisations belong here, as do groups that represent them and any reporting/commentary specifically targeted on this area. Note that IT-related businesses belong to the 'Computers & Internet' category and are not included here.	Allow	Allow	Allow
Computing & Internet	All sites related to computer hardware and software - including sales. News and current trends regarding the computing industry or internet are also applicable. Professional bodies within the IT industry are included. Please note that sites whose main function is to allow users to download software are listed in the 'Software Download' category.	Allow	Allow	Allow
Drugs	Sites that sell illegal/controlled substances, promote substance abuse, or sell related paraphernalia.	Denied	Denied	Denied
Education	Colleges, universities, primary and secondary schools are all listed here. Online educational resources, such as exam syllabuses and example questions, are also included. Support organisations such as admissions bodies and research councils.	Allow	Allow	Allow
Finance & Investment	All aspects of personal and corporate finance are included here. Sites that provide price comparisons between financial products. Sites that report or comment on financial matters.	Allow	Denied	Allow
Food & Drink	All sites relating to restaurants (whether eat-in or takeaway) and pubs/bars. All recipes and cuisine related sites are listed in this category. Farms and other foodstuff manufacturers.	Allow	Allow	Allow
Gambling	All online and offline gambling, and sites that promote gambling skills and practice.	Denied	Denied	Denied
Gaming	All sites relating to video, computer or online games. All sites that support gaming through hosting online services, cheat information, general advice etc.	Denied	Denied	Denied
Government	All central and local government websites are applicable,	Allow	Allow	Allow

	as are related bodies and agencies. Sites related to defence forces such as armies, navies or air forces are not included here -they are listed in the 'Military' category.			
Hacking	Resources for the illegal or questionable use of computer hardware or software are listed here, as are sites that promote destructive or malicious software such as viruses and trojans. Sites that describe how to gain unauthorized access to systems. Sites that distribute copyrighted material that has been 'cracked' to bypass licencing.	Denied	Denied	Denied
Hate & Discrimination	Sites promoting aggressive, degrading, or abusive opinions about any section of the population that could be identified by race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice. Political and social groups that discriminate on the grounds of race, religion, gender, age, nationality, physical disability, economic situation, sexual preferences or any other lifestyle choice.	Denied	Denied	Denied
Health	All sites related to personal health, hospitals, clinics, legally-prescribed medication and related services.	Allow	Allow	Allow
Illegal	Sites that contain instructions, recipes, or advice on creating illegal items, such as explosives, or offer them for sale. Sites that give instruction on, advice about or promote of illegal acts.	Denied	Denied	Denied
Image Sites	Sites that provide hosting for images.	Allow	Denied	Denied
Instant Messaging	Instant messaging clients and services, and any domains required for their successful operation.	Allow	Denied	Allow
Internet Telephony	All sites that offer internet telephony/VoIP products and services.	Allow	Denied	Allow
Lifestyle & Culture	Sites that deal with life issues such as motherhood and raising children. Life events such as marriage and bereavement. Lifestyle choice sites such as gay/lesbian/bisexual are listed here. Sexual content is explicitly excluded and is listed in 'Pornography & Adult Content'.	Allow	Allow	Allow
News	All reporting media such as online news, newspapers and current affairs sites are listed here.	Allow	Allow	Allow
Newsgroups & Forums	Sites offering access to Usenet newsgroups or similar services, or any other discussion forum that doesn't sit well in another category.	Allow	Denied	Allow
Offensive & Tasteless	It's not very easy to define exactly what is offensive or tasteless. Sites included are not pornographic or violent;rather, more oriented towards content unsuitable for school children to view or that an employer would be uncomfortable with their staff accessing. Some examples are: discussion of sexual activity of a non-pornographic but explicit fashion; crude humour; images of the casualties from a car crash; defamatory or insulting comments about people, places, religions or cultures.	Denied	Denied	Denied
Peer To Peer	All sites that facilitate the sharing of files using P2P software are placed in this category. This includes, but is not restricted to, sites that host P2P software and sites that allow users to search for files that can be downloaded using via P2P software.	Denied	Denied	Denied
Dating	This category covers matchmaking sites, personal listings, sites that discuss romance and interpersonal relationships	Denied	Denied	Denied

	-whether partnership is the resultant goal or not. Sites specifically designed for initiating sexual encounters are excluded -these are categorised as 'Pornography & Adult Content'.			
Pornography & Adult Material	Sites containing sexually explicit content in an image-based or textual form. Any other form of adult/sexually-oriented material is also listed here. For example: Escort agencies and swingers clubs; "	Denied	Denied	Denied
Property & Real Estate	All sites oriented to the selling, letting, and building of private or commercial property should be placed in this category.	Denied	Denied	Denied
Proxy Avoidance	Any site that operates as a web proxy, allows access to software that can bypass web filtering, or offers guidance on how web filtering can be avoided is listed in this category.	Denied	Denied	Denied
Recreation & Hobbies	This category covers all activities or interests, other than sport, that someone might pursue for their own pleasure and not as a main occupation. This is obviously a very broad definition	Allow	Denied	Allow
Recruitment	All employment agencies, recruitment consultancies and headhunters, contractors, and agencies assisting anyone seeking employment are placed here. All sites that allow job vacancies to be posted, offer career advice, describe how to get through interviews or prepare a CV.	Allow	Allow	Allow
Reference	Online encyclopaedias, dictionaries, thesauruses, atlases and other information resources available for research purposes all belong to this category.	Allow	Allow	Allow
Religion	All sites that relate to religious belief or scepticism should be placed in this category.	Allow	Allow	Allow
Search Engines	This category contains all search engines, meta-search engines and web directories.	Allow	Allow	Allow
Sex Education	This category exists to allow users to access site that discuss sex and sexuality in an informative and non-voyeuristic way. Topics that fall under this category include: education about human reproduction and contraception, sites that offer advice on preventing infection from sexual diseases such as HIV, and sites that offer advice to the LGB communities on sexual health matters.	Allow	Allow	Allow
Shopping	Any site that meets one of the following criteria is listed here: Offers goods for sale; represents a non-online retailer; provides comparisons between goods; preferential purchase schemes. Please note that exceptions are made in the case of sites covered by the other categories: auctions, cars and spares, sexual goods and materials, computer hardware and software, computer and video games, holidays and travel, financial goods and services, alcohol and tobacco, drugs, prescription medicines and weaponry -these are all be placed in the category best suited to the specific purpose.	Allow	Denied	Allow
SMS & Mobile Telephony Services	This category is used for sites that allow the creation or sending of SMS text messages. Sites that sell ringtones, games, videos, or other downloadable content. Please note that mobile telephone retailers are not placed in this category -they are listed in 'Shopping'.	Allow	Denied	Allow

Software Download	All sites whose main purpose is to allow users to download software, whether on a free or commercial basis.	Allow	Denied	Allow
Sport	All sport websites -whether official, unofficial, media-related or fan-related -are placed in this category, except for those related to gambling.	Allow	Denied	Allow
Streaming Media & Media Downloads	Any site whose primary function is to allow users to download media content, whether streamed or not.	Allow	Denied	Allow
Translation	All sites that translate a web page from one language to another, or that transform the text contained within a web page, are listed in this category.	Allow	Allow	Allow
Travel	Sites related to the following topics are listed here:-Travel agents.-Airlines, cruise and ferry lines, rail operators, bus and coach companies.-Hotels and holiday rental accommodation. -Travel advice.-Timetable information.-Car hire.	Allow	Allow	Allow
Violence	Any site that displays or promotes content related to violence against humans or animals isplaced in this category, as are sites that advocate any means of harming oneself such as self-mutilation or euthanasia.	Denied	Denied	Denied
Weapons	Any site that sells weapons or ammunition or advocates the use of weapons. Sites of weapons manufacturers.	Denied	Denied	Denied
Webchat	Web-based chatrooms.	Allow	Denied	Allow
Weblogs & Social Interaction	Any site that hosts a weblog or lists of weblogs, or provides social networking services is listed in this category. Social networking sites are defined as those that allow users to generate their own profiles or personal content, view the profiles of others, and create links between profiles in order to indicate friendship or approval.	Allow	Denied	Allow
Spyware	Websites hosting software that attempts to get hold of personal or secret information without the users knowledge.	Denied	Denied	Denied
Webmail	Any site offering web-based email services is placed in this category.	Allow	Denied	Allow

King William's College & The Buchan School

Social Media Policy

Issue Date: 02/15

Date Reviewed: 03/19

Next Review Date: 03/21

Stuart Corrie

Deputy Head Pastoral

Introduction

For the purposes of this document, Social Media is defined as any category of online media that supports groups and individuals communicating, participating, sharing, networking and bookmarking online. Common social media platforms include, but are not limited to: online social networks such as Facebook, LinkedIn and Twitter; blogs, podcasts and discussion forums; RSS feeds and content sharing sites such as Instagram and YouTube.

The importance of teachers, students and parents engaging, collaborating, learning, and sharing in these digital environments is integral to 21st century learning. To this aim, King Williams College has introduced the following policy to provide direction for all staff when participating in online social media activities particularly, but not exclusively, during the school working day.

The purpose of this policy is to help protect both the school and the personal interests of staff. The aims of this document are:

- To provide clarity to staff on the use of social media tools when acting independently or as a representative of King William's College

- To ensure that the reputation of King William's College is not brought into disrepute

- To ensure that internet users are able to distinguish between official school information and the personal opinions of staff.

1. General Social Media use

1.1 Many staff members already use social media, particularly interactive and collaborative websites, both in a personal and professional capacity. Rather than try to restrict this activity, King William's College aims to provide guidance which will enable staff to interact online in a way that is credible, consistent, transparent and relevant.

1.2 Posts made through personal accounts may breach this policy if they bring the organisation into disrepute. This includes situations when an individual could be identifiable as a King William's College employee whilst using social networking tools, or occasions when commenting on school related matters in a public forum.

1.3 If a staff member does identify themselves as an employee of this organisation then they should ensure that their profile and related content is consistent with the image they wish to present to colleagues and what the school would deem appropriate. Staff should not operate online in a way which could call into question their position as a professional.

1.4 Staff should not post content that may attract negative attention and should be mindful of the way they express themselves and of the risk that comments may be taken out of context.

1.5 Staff may not upload images containing students into any social media forum, except with the prior approval of the SMT to officially sanctioned school forums.

1.6 Staff should not engage in discussion/debate or offer information to the media in a representative role. Staff must at all times refer enquiries from the media to the Principal.

1.7 Staff should not, at any point, include anything that could be considered offensive or discriminatory to any individual, or deemed as bullying or harassment of any individual. Examples include but are not limited to:

      1.7.1   Making offensive or derogatory comments relating to sex, gender, race, sexual orientation, religion or belief

      1.7.2   Using social media to bully another individual or make comments likely to be perceived as of a bullying nature

      1.7.3   Posting images that are discriminatory or offensive or links to such content.

2. Personal use of social media at work

2.1. Staff are not allowed to access social media websites from the school's computers or devices at any time during the school working day. Whilst it is understood that staff may wish to use their own devices to access such media whilst at school, staff must limit their use to non-contact time (such as breaks, lunch and after school).

2.2. If it is believed that a member of staff has engaged in any activity in breach of this policy and the school contract, then an investigation may be instigated which could result in disciplinary action.

3. Use of social media and the Internet for work purposes

In specific circumstances it may be appropriate for a member of staff to use social media as part of their work. There must, however, be a strong pedagogical reason for creating official media sites to communicate with pupils or others. Such sites should only be created with the written approval of the Principal, Vice-Principal or their designated representative. In such circumstances the same safeguards must be adhered to as would be expected with any other form of communication about the School in the public domain. Any communications made in a professional capacity through social media must not either knowingly or recklessly:

3.1. Bring the school into disrepute

3.2. Breach confidentiality

3.3. Breach copyright

3.4. Breach data protection legislation

3.5. Communicate inaccurate or inappropriate information to students, staff or parents. (Social media is not considered to be an appropriate forum to communicate official information, with the exception of officially approved groups (such as Tour group pages) or the official school sites.

3.6. Involve interaction with pupils via social media/Internet sites without appropriate authorisation.

3.7. Involve interaction with any ex-student who is under the age of 18 (staff should exercise caution in interacting with any ex-pupils regardless of age)

The above is a non-exhaustive list and is intended to provide some examples of what we consider to be inappropriate. If in any doubt, staff should consult with their line manager or Head of Department.

4. Use of social media in your personal life

We recognise that many members of staff make use of social media in a personal capacity. Please therefore bear in mind the following guidelines:

4.1. Any communications made in a personal capacity through social media must not bring the School into disrepute. Staff should avoid distribution of images or other media that may create a negative impression or cast doubt on the professionalism of the individual or the school.

4.2. Staff may identify that they work for a school, but their online profile or name (such as the name of a blog or a twitter account name), or the name of a page or website, must not contain the School's name as part of the title, with the exception of officially approved groups.

4.3. If discussing work on social media (for example, giving opinions on a subject specialism etc), where appropriate a disclaimer should include a statement along the lines of: "The views I express here are mine alone and do not necessarily reflect the views of the School".

4.4. Whilst close family ties or other circumstances will create exceptions, it is strongly advised to avoid online interaction with any student who is under the age of 18, (staff should exercise extreme caution in interacting with any ex-pupils regardless of age).

4.5. Consider the language used by contacts in association with the member of staff's name.

4.6. Members of staff are strongly advised to ensure privacy settings are set to their strictest levels.

5. Disciplinary action over social media use

All staff members are required to adhere to this policy. Staff should note that any breach of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing damage to the reputation of the School, may be deemed to constitute gross misconduct.