St Patrick's Academy, Dungannon

E-SAFETY POLICY

'Achieving Excellence Together'

June 2024

Introduction

St Patrick's Academy is committed to providing a safe and caring environment for all of our pupils. School ICT resources are intended to be used for educational and work-related purposes only. We are committed to supporting any pupil or staff member who experiences bullying type behaviour online or through the inappropriate use of a digital communication device. We recognise that the well-being of our school community is of paramount importance and we aim to promote positive relationships between pupils, parents/carers and staff so that everyone can feel comfortable in reporting e-safety concerns and be confident that they will be dealt with promptly, effectively and confidentially.

Aims

The purpose of this policy is to establish the rules regarding the appropriate use ICT equipment and the internet in school, when pupils are in uniform outside of school and when pupils are on school-related business such as trips and events. In St Patrick's Academy, we will:

- Provide opportunities for pupils to use digital and information technologies safely and appropriately;
- Promote the use of ICT to stimulate discussion, promote creativity and increase opportunities for learning in a structured and supervised manner;
- Have necessary safeguards in place such as educating our parents and pupils through the use of guest speakers, weekly assemblies, robust policies, user agreements and effective PD lessons;
- Follow the school's Safeguarding Policy so that all reported incidents are dealt with consistently, effectively and efficiently.

Roles and responsibilities

Board of Governors will:

- Maintain an oversight of the E-Safety Policy, ensure its effective implementation and review the policy annually;
- Be kept informed of e-safety incidents by the Principal and, when appropriate, of sanctions applied;
- Identify trends and priorities for action by including e-safety as an item for discussion on agendas;

The Principal and members of SLT will:

- Consult with the school community when drawing up and reviewing our e-safety policy;
- Appoint an E-Safety Officer who will have the day-to-day responsibility for e-safety within the school;
- Ensure that the E-Safety Officer is supported in their work and to ensure that effective monitoring systems are in place so that all of members of the school community feel safe;
- Be aware of potential child protection issues which may arise and ensure that members of the Safeguarding Team are alerted and have received appropriate training;
- Accurately record all incidents and alleged incidents of e-safety breaches using the Behaviour Management Module;
- Review the effectiveness of the policy in conjunction with the E-Safety Officer;
- Provide training for all staff as and when the need arises.

The E-Safety Officer will:

- Liaise with appropriate staff including the Principal, Designated Teacher and those in Charge of Digital Communications to ensure that the school's infrastructure is secure and that filtering and password policies are up-to-date;
- Ensure that all staff are aware of the procedures to follow in the event of an e-safety incident;
- Support staff when dealing with an e-safety issue and keep an accurate record of all incidents using the school's Official Record Book;
- Monitor and review the e-safety education programme for the school and provide appropriate resources for the PD programme ;
- Provide resources for assemblies on, for example, Internet Safety Week;
- Identify the needs of staff and provide appropriate training opportunities.

Staff (Teaching and non-teaching) will:

- Have read and understood the Staff Acceptable Usage and E-Safety Policies;
- Promote and monitor the effective use of ICT within the classroom;

- Provide carefully planned lessons so that pupils are not subjected to unsuitable material found in internet searches;
- Be vigilant when supervising pupils using communication devices during their lesson or when on duty;
- Intervene to support any pupil experiencing bullying-type behaviour online and report any concerns to the E-Safety Officer;
- Follow school policy with regard to safeguarding and partake in any training provided;
- Provide guidance to pupils in order to avoid plagiarism and copyright issues.

Pupils will:

- Follow the instructions given by their teacher;
- Ensure that parents are shown Pupil Acceptable Usage Policy in their planners;
- Report any worries or concerns they may have to their tutor, Head of Year, E-safety Officer or Vice-Principal;
- Keep mobile devices switched off and kept out of sight while on the school premises unless they are being used to facilitate online learning and with a teacher's permission. Any pupil failing to do so will have their device confiscated and a parent/carer must collect it from the Principal's PA.
- Never use their iPod/iPad/phone to record an image (video or still) or to make an audio recording of a pupil or member of staff. Anyone caught doing so, or attempting to do so, will be suspended. Anyone who forwards or posts and image or recording will also be suspended. In addition, anyone caught trying to provoke a situation whereby a video or audio recording will be made will be suspended;
- Participate in the school's E-Safety Programme and to respect and follow guidelines given by their teachers in relation to copyright.

Parents will:

- Read, with their child, the Pupil Acceptable Usage Policy in planners and sign it alongside their child's signature each year;
- Inform the school of any concerns they may have relating to e-safety.

Communication

- Digital tools such as Google Classroom should be used professionally and only used to conduct school business.
- The school's e-mail service should be accessed via the provided web-based interface by default.
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using their personal e-mail addresses.
- Teachers should never communicate with a parent directly using their email address. The school's 'info' account can be used, if necessary.
- School e-mail is not to be used for personal use.
- Pupils must not use their mobile phone in school unless directed to do so by their teacher. A phone line is available in the school office if any pupil needs to contact home. Parents/carers are asked not to communicate with their child via mobile phone during the school day and should contact the school's Reception Desk instead.
- Staff should not use their mobile phones during working hours when in contact with pupils.

Social Media

- Pupils are not allowed on social networking sites when in school. Parents should be aware that it is illegal to access certain social media sites under the age of 13.
- Staff should not access social networking sites on school equipment, in school or at home. Staff should access sites using personal equipment.
- Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog.
- Students/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students and/or staff.
- If inappropriate comments are placed on social networking sites about the school or school staff, advice may be sought from the relevant agencies, including the police, if necessary.
- The school will use social media in a positive way to inform, publicise school events and celebrate and share the achievement of students.

- Students in KS3 will be taught about e-safety issues on social networking sites as we accept that some may use them outside of school.

Digital Images

- The school's record of parental permissions should be adhered to when taking images of our students. Permission will be contained within the school's intake form. Pupils who do not have permission will be noted on the school's Information Management System e.g. SIMS/BROMCOM
- Under no circumstances should images be taken on privately-owned equipment unless permission has been granted by the Principal. Where permission has been granted, these should then be transferred to the school's storage repository and deleted from the privately-owned device.
- Images taken on a school device should also be stored in the school repository. These images should be kept for no longer than is necessary and then deleted.
- The Teacher in Charge of Digital Learning and the E-Safety Officer will carry out an annual audit of digital images and delete those which are no longer needed.
- Permission to use images of all staff who work at the school is sought on induction.

Websites

- Staff will preview any websites before recommending them to pupils. Pupils should only access these recommended websites.
- Open searching of websites should be discouraged as younger pupils may misinterpret information.
- When a pupil is carrying out research from home, staff will only recommend sites that have been checked. Parents will be advised to supervise any further research.
- Staff have a role in checking material a pupil has viewed.
- Pupils must observe copyright of materials published online.
- In consultation with the Principal or Vice-Principal, only the E-Safety Officer, Teacher in Charge of Digital Communications or any member of the Safeguarding Team can check internet logs.

Passwords

- Passwords or encryption keys should not be recorded on paper or in an unprotected file. Passwords should be changed at least every 3 months and users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems.
- Passwords should never be shared with anyone.
- Pupils should inform staff immediately if their password is traced or forgotten or if their school account has been 'hacked'.

Use of School Equipment

- Privately-owned equipment, applications or packages should never be connected to the school's network without permission from the E-Safety Officer and in line with the school's BYOD policy (Appendix 6).
- Staff and pupils should never store personal or sensitive data on school equipment or local drives.
- Staff should 'lock' their screen or log off before moving away from their computer.
- All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the E-Safety Officer or an appropriate member of SLT.
- An appropriate member of SLT will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems.

Incidents of misuse

It is hoped that all members of the school community will use ICT responsibly. All staff will be asked monitor the use of ICT by their pupils but will pass on e-safety concerns to the E-Safety Officer or the school's Safeguarding Team. Our response to misuse (appendix 2) will be in line with school policy. More than one member of staff will be involved:

- Inappropriate misuse of ICT will be referred to the E-Safety Officer who will inform the Head of Year (appendix 3);
- All safeguarding concerns will be passed to the E-Safety Officer and Designated/Deputy Designated Teacher;
- Illegal misuse will be referred by the E-Safety Officer directly to the Principal (appendix 4).

Bring Your Own Device (BYOD)

BYOD means privately-owned portable equipment such as laptops, tablets, ultra-books, smart phones/watches, cameras and any device capable of accessing the internet. BYOD users must abide by the following rules:

- Use the internet connection provided by the school;
- Use the technology for educational purposes only;
- Must be virus-protected and not capable of passing on any infections;
- Must be charged at home;
- Sign the Acceptable User Agreement as provided by the school.

Full BYOD Policy is in Appendix 7.

Online Lessons

- Online forums should be used for educational purposes only;
- Teachers should not communicate one-to-one with a pupil online;
- Cameras/microphones should be switched on at the beginning of the lesson;
- Pupils should be appropriately dressed and in a public living area – bedrooms and bathrooms are not permitted;
- Pupils should engage as if they were in the classroom and maintain the standard expected of the school;
- Pupils must not share passwords or invite other students to join the lesson;
- Pupils must not record or distribute any part of the online lesson;
- Pupils not using online lessons for the intended purpose will be removed from future lessons and a sanction applied.

Use of mobile phones

St Patrick's Academy recognises that mobile phone technology can play an important role in teaching and learning. We also appreciate that students often carry mobile phones so that they can contact parents before and after school.

If students are entrusted to carry mobile phones with them for use before and after school, the following should be noted:

- Mobile phones must be switched off at all times during the school day, including at buses, during break and lunchtimes. They must remain off whilst students are on the school premises unless directed to do otherwise by a teacher. It is not acceptable for phones to be put on silent;
- The phone must be kept out of sight during lessons;
- No student may take a mobile phone into a room or other area where examinations are being held;
- The security of the phone will remain the student's responsibility in all lessons including PE/gym lessons;
- The pupil phone at reception should be used if a pupil needs to contact a parent/carer.

Breaches

Misuse of a mobile phone will be dealt with as a serious breach of the student commitment and will be dealt with in line with the school's Safeguarding Policy in relation to electronic communication devices. 'Misuse' will be at the discretion of the principal, vice-principals and E-Safety Officer of the school. Some examples of misuse include:

- sending inappropriate messages;
- sending inappropriate messages or posts to social networking or blogging sites;
- taking photographs and/or videos in school;
- photographing or filming staff or other students;
- photographing or filming in toilets, changing rooms and similar areas;
- bullying, harassing, humiliating or intimidating staff or students by the use of text, email or multimedia messaging;
- refusing to switch a phone off or hand over the phone at the request of a member of staff;
- using the mobile phone outside school hours to intimidate or upset staff and students will be considered a breach of these guidelines;
- using a mobile phone outside school hours in such a way that it undermines the stability of the school and compromises its ability to fulfil the stated aim of providing 'a clear moral and ethical lead';
- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience such as on SnapChat, BeReal, WhatsApp or any other platform;

- bullying behaviour by text, image, and email messaging
- the use of a mobile phone for 'sexting' (the deliberate taking and sending of provocative images or text messages);
- posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to other;
- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other students, this will include the manipulation of images to superimpose someone's face, body or voice onto something else;
- general disruption to learning caused by students accessing phones during lessons;
- students phoning parents;
- students phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised;
- publishing photographs of vulnerable students, who may be on a child protection plan, where this may put them at additional risk.

Dealing with breaches
Misuse of a mobile phone in school will usually be sanctioned with a suspension, however, the school may consider the intent, context and person targeted before applying this sanction. Serious misuse may include the student being internally or externally excluded from school. If the offence is serious, it will be reported to the PSNI.

Where a mobile phone is confiscated, it will be stored safely and securely with the Principal's PA where the confiscation will be recorded, and the parent contacted. Where a student persistently breaches the expectations, following a clear warning, the principal may impose an outright ban from bringing a mobile phone to school. This may be a fixed period or permanent ban.

Confiscation procedure
When a mobile phone is confiscated, it should be switched off, brought directly to the Prinicpal's PA and placed in an envelope with the time/date recorded. A log of confiscations will also be kept. The phone will be stored safely and securely until a parent is able to collect it. The Principal's PA will contact the parent/guardian immediately to inform them of the confiscation.

Sanctions
In line with the school's Safeguarding Policy, students and parents will be notified if appropriate action needs to be taken against those who are in breach of the acceptable use guidelines.

In addition:

- Students and their parents should be very clear that the school is within its rights to confiscate the phone where the guidelines have been breached;
- If a phone is confiscated, it will require a parent/carer to sign for and collect the phone from school;
- Students should be aware that the PSNI will be informed if there is a serious misuse of the mobile phone such as where criminal activity is suspected;
- If a student commits an act which causes serious harassment, alarm or distress to another student or member of staff, the ultimate sanction may be exclusion. The school will consider the impact on the person experiencing the negative behaviour in deciding the sanction.

In accordance with the school's E-Safety Policy and in line with the Addressing Bullying in Schools Act 2016, we treat the misuse of electronic devices seriously, especially when posts are detrimental to pupils' attendance, relationships, emotional well-being, and learning. When socially unacceptable online behaviour happens in or on the way to school, and/or on an authorised school platform such as Google Classroom or C2K email, the school will apply an appropriate consequence in line with our Code of Conduct and will support all pupils affected and involved. If an incident of cyber bullying type behaviour takes place outside school and impacts negatively on the social and emotional well-being of a pupil/s in school, we will act in line with legislation to investigate the incident, support all involved and raise awareness of safe, responsible, respectful internet usage. Some of the actions we will take include:

- informing parents/carers;
- supporting those experiencing and displaying the socially unacceptable/bullying type behaviour by completing a programme of restorative/educative work;

- addressing key themes of online behaviour and risk through PD, LLW, Form Class lessons, Year and Key Stage/Whole School Assemblies;
- engaging with key statutory and voluntary sector agencies (e.g., C2k, PSNI, Public Health Agency, Safeguarding Board for NI) to support the promotion of key messages;
- participating in annual Safer Internet Day and the promotion of key messages throughout the year about how to respond to harm and the consequences of inappropriate use.
- developing, implementing, and reviewing robust and appropriate policies in related areas such as E-Safety, Acceptable Use of ICT and Mobile Phone policies.

Review

The school will carry out a review of the E-Safety Policy every year.

Linked Documents

Addressing Bullying Policy
Bring Your Own Device Policy
Child Protection Policy
ICT Policy
Positive Behaviour for Learning Policy
Safeguarding Policy

Reviewed: June 2024
To be reviewed: June 2025

Appendix 1 - Communications

A wide range of technologies have the ability to enhance learning. The table below outlines technologies that can be used in school

	Staff and other adults				Students and young people			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to school	✓				✓			
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photographs on mobile devices				✓				✓
Use of other educational mobile devices	✓						✓	
Use of school email for personal emails				✓				✓
Social use of chat rooms / facilities				✓				✓
Use of social network sites			✓				✓	
Use of educational blogs	✓				✓			

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users should be aware that email communications may be monitored
- Users must immediately report, to the c2K manager 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 pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Appendix 2 – Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes 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:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Criminally racist material					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
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				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards on the school system				✓	
Uploading, downloading or transmitting 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)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 3 - Student Disciplinary Procedures

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to HOD / Principal and/or e-safety officer**	**Refer to police**	**Refer to technical support staff / c2K Manager for action e,g, security/ filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device including smart watches	✓			
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	✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓		✓
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		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

Appendix 4 - Staff Disciplinary Procedures

Incidents involving members of staff	**Refer to the Principal** ***See below**	**Refer to technical support staff / C2K Manager for action re filtering, security etc**	**Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access 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 e.g. 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	✓		✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓		✓
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	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

***In event of breaches of policy by the Principal, refer to the Chair of Governors.**

Appendix 5 - Acceptable Use Policy for Pupils

This document is a guide for young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone / IPod) in school at times that are permitted; commuting to and from school, or to contact parents after participation in an extra- curricular activity. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Pupil Signature ……..

Parent Signature ……..

Date …….

Appendix 6 - Acceptable Use Policy for Staff

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 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.
- 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 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.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, I Pad's etc.) out of school
- I understand that the school 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 school.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission
- 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
- 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 school's policy on the use of digital/video images. I will not use my personal equipment to record these images
- I will only use chat and social networking sites in the school in accordance with the school's policies

- I will only communicate with student and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities

St. Patrick's Academy and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (laptops/I Pad's, mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems
- 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
- I will ensure that my data is regularly backed up, in accordance with relevant policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography) 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
- 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
- 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 allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the schools policies. Where personal data is transferred outside the secure network, it must be encrypted
- I understand that data protection policy requires that any staff or learner 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
- I will immediately report any damage or faults involving equipment or software, however this may have happened

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

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

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

- I understand that this Acceptable Use Policy applies not only to my work and use of 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

- I understand that if I fail to comply with this Acceptable 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

I have read and understand the above and agree to use St. Patrick's Academy 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 ……..

Appendix 7 - BRING YOUR OWN DEVICE (BYOD) POLICY

St Patrick's Academy Dungannon

Rationale

Sixth Form students have access to a limited number of private study periods during which they have the opportunity to focus on coursework, homework tasks and assignments. Traditionally much of this work has been completed using pen and paper. As the nature of exam courses change and more materials are made available in digital form, students are increasingly required to use and to produce materials in digital form to aid learning. The school recognises the benefits to learning from offering Sixth Form students the opportunity to use personal ICT devices in school to support learners and their learning. It is the intention of this policy to facilitate and support the use of personal ICT devices in school in furtherance of individualised student learning. Sixth Form students are expected to use personal ICT devices in accordance with this policy and must sign a declaration agreeing to be bound by the additional school rules and requirements set out in this policy before they will be permitted to use personal ICT devices in school.

Guidelines for Acceptable Use of Personal ICT Devices

- The use of personal ICT devices falls under **St Patrick's Academy Dungannon Internet Acceptable Use Policy** which all students must agree to, and comply with.
- The primary purpose of the use of personal devices at school is **educational**. Using the device for personal reasons should only take place after permission has been given from a teacher or other member of staff.
- Students **are not permitted to connect to any wireless or networking service** other than the schools trusted C2KNI network while using a personal ICT device in school.
- Use of personal ICT devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher.
- The use of a personal ICT device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt class or Private Study areas in any way. Playing games or other non-school work related activities are not permitted.
- Students shall only use a personal ICT device while under supervision in a Private Study room or a subject classroom unless otherwise directed by a teacher e.g. on school visits or activities.
- Students shall make no attempts to circumvent the school's network security. This includes setting up proxies and downloading programs to bypass security.
- Students shall not distribute pictures or video or any other material relating to students or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).
- Students must check their personal ICT device daily to ensure the device is free from unsuitable material and free from viruses etc. before bringing the device into school.

- Students must check their personal ICT device daily for basic Health and Safety compliance to ensure it is free from defects. Particular attention should be paid to the power lead (lead not frayed; plug correctly fitted and containing the correct fuse rating), the keyboard (all keys present; no bare metal exposed), the screen (free from flicker and damage) and the device battery (able to hold a charge). Any personal ICT device that has obvious Health and Safety defects should not be brought into school

Consequences for Misuse/Disruption

In addition to dealing with misuse/disruption within the remit of St Patrick's Academy Acceptable Use of the Internet Policy and the school's Positive Behaviour Policy one or more of the following sanctions may apply:

- Personal ICT device would be confiscated and kept in the front office until parent/guardian picks it up.
- Privilege of using personal ICT devices at school would be removed.
- Serious misuse of Internet capable devices is regarded as a serious offence in direct contravention of St Patrick's Academy Dungannon **Bring Your Own Device (BYOD) Policy, the Internet Acceptable Use Policy** and the **Positive Behaviour Policy** and will be dealt with in accordance with these policies.

School Liability Statement

Students bring their personal ICT devices to use at St Patrick's Academy Dungannon **at their own risk.** Students are expected to act responsibly with regards to their own device, **keeping it up to date via regular anti-virus and operating system updates** and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

St Patrick's Academy is in no way responsible for:

- Personal devices that are broken while at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
- Parents should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal ICT device in the event of loss/damage to the device.

- **Bring Your Own Device - User Agreement Student Declaration**

- I would like to use my own personal ICT device in school. I confirm this device is on the approved list of devices including laptops, tablets and iPads. I have read and understood the Bring Your Own Device Policy (BYOD) and I agree to be bound by the guidelines, rules and regulations contained in the BYOD policy, the Internet Acceptable Use Policy and the Positive Behaviour policy. I understand that the use of a personal ICT device in school is a privilege, not a right and agree to use the device for learning only. I agree to only connect to our school's wireless networking service while using my personal ICT device in school. I understand that I am solely responsible for the correct care, safety and security of my personal ICT device when in school.

- **Print Name: _____Class: _____**
- **Signed: _____ Date: _____**

Parent/Guardian Approval

- *Disclaimer - please read carefully*
- St Patrick's Academy Dungannon accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school-sponsored activities. The decision to bring a personal ICT device into school rests with the student and their parent(s)/guardian(s), as does the liability for any loss/damage that may result from the use of a personal ICT device in school. It is a condition of agreeing to allow students to bring personal ICT devices into school, that the parent/guardian countersigning the permission slip accepts this disclaimer.
- I have read the **Bring Your Own Device Policy (BYOD)** and give my son/daughter approval to use a personal ICT device in school. I understand my son/daughter is personally and solely responsible for the **correct care, safety and security of the device.** I understand that the school accepts no liability in respect of any personal ICT device used in school by a student. I understand and accept the disclaimer.

- Signed: _____(Parent/Guardian) Date: _____