St. Patrick's Grammar School ARMAGH

E-Safety Policy

The aim of this E-Safety policy is to ensure that pupils will benefit from learning opportunities offered by the school's electronic resources in a safe and effective manner. E-Safety covers issues relating to pupils and their safe use of the Internet, mobile phones and other electronic communications technologies, within school. Internet use and access to other electronic media is considered a school resource and privilege. Therefore, if the school's E-Safety Policy is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed.

Internet Use – Teaching and Learning

Internet use is part of the statutory curriculum and is a necessary tool for learning. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in school is to:

- raise educational standards
- to promote pupil achievement
- to support the professional work of staff
- to enhance the school's management functions

Internet access is an entitlement for students who show a responsible and mature approach to its use. Through the school curriculum and discrete ICT classes pupils will be taught:

- What Internet use is acceptable and what is not.
- The effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- To acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Internet Filtering

The school uses the C2K Internet filtering system which provides an effective defence against inappropriate websites. C2K define three types of access:

- **GREEN** – accessible to all users in schools
- **AMBER** – accessible to school's selected groups of users (can be changed by the C2K Manager)
- **RED** – not accessible to any user

An Internet filtering service, no matter how thorough, can **never** be comprehensive. To deal with this issue the school enforces the following rules/procedures:

- Internet sessions will be supervised by a member of staff where possible.
- Pupils' Internet usage is regularly monitored
- Students will be aware that any usage, including distributing or receiving information, may be monitored for unusual activity, security and/or network management reasons.
- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students and Staff will report accidental accessing of inappropriate materials in accordance with school procedures.

If staff or pupils discover unsuitable sites, the URL will be reported to the C2K Manager or the Network Manager who will then inform the C2K filtering team to block this website.

The school will work with the C2K team to ensure that the filtering policy is continually reviewed.

Email

Email is an essential means of communication for both staff and pupils for school related business only. The school uses the approved filtered email service provided by C2K. E-mails containing offensive material will immediately be sent to the Prinicpal for further investigation. The investigation will be in accordance with other related school policies and may involve outside agencies. The following email procedures are enforced in school:

- Students will use approved C2K email accounts under supervision by or permission from a teacher. Access to other email accounts will be blocked.
- Students and staff will not send or receive any material that is illegal, obscene or defamatory or that is intended to annoy or intimidate another person.

- Students and staff will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will be encouraged not to arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Students must immediately tell a member of teaching staff if they receive offensive email.

Computer Network Security

The school currently operates two computer networks: C2k and Legacy. The C2K network is managed and maintained by the C2K support team in the SELB along with Northgate who is responsible for the hardware and the security of the system.

The Legacy network is maintained within the school by the Network Manager. The following protocols are enforced by the school to comply with security regulations:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media will be scanned with anti-virus / malware software. Any device which has a virus will be denied access.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

Social Networking

Social networking sites can connect people with similar or different interests but can also pose a number of dangers. All staff and students will be made aware of the potential risks of using social networking sites outside of school. They will be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their status.

Social Networking sites such as Facebook, Bebo, Twitter and MySpace are all blocked by the C2K Internet filter. However, due to the educational value of Wikis and Blogs, only approved,

secured and monitored sites are allowed through the filter such as PBWiki and 21 Classes. Staff are advised and given technical support to help set up a secure Wiki and Blog within school and are shown how to monitor the site appropriately. All students who use the Wiki or Blog within school will be assigned usernames and passwords by the teacher to ensure security. Access to the Wiki or Blog within school is strictly for educational purposes only and anyone wishing to join the workspace who is not an approved member by the teacher moderator will be denied access.

The following guidance is given to **all** members of the school community regarding the use of social networking sites which should only be accessed outside of school hours:

- Never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff educational Blogs or Wikis should be password protected and are asked to monitor the site very closely. Any breach in security or inappropriate material being published should be immediately reported to the Senior Management Team.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory or bring the name of St Patrick's Grammar School into disrepute. Criminal proceedings may be brought to bear in cases where this rule has been contravened.
- Concerns regarding students' use of social networking, social media and personal publishing sites (out of school) will be raised with their parents/carers if it impacts on the school community.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff training days and will be outlined in the Staff Code of Conduct.
- Students who access social networking sites blocked by C2K on their mobile phones during school hours are in breach of the school rules. The school's positive behaviour policy will be followed.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone"

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying. There are clear procedures in place to support anyone in the school community affected by Cyberbullying:

- All incidents of Cyberbullying reported to the school will be recorded.
- All incidents or allegations of Cyberbullying will be fully investigated.
- Pupils, staff and parents/carers will be advised to keep a written record of the bullying as evidence.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to Cyberbullying and the school's e-Safety ethos.

Electronic devices

Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

The school employs a strict policy on the use of mobile phones on school premises between 8.50 a.m. and 3:30 p.m. Guidelines and sanctions are outlined in the school's mobile phone policy. The following points outline the e-safety guidelines for mobile phones:

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy and may also be a criminal offence.

- Mobile phones and personal devices will not normally be used during lessons or formal school time unless under the direction of a member of staff for educational purposes.
- The Bluetooth function of all devices should be switched off at all times and not be used to send images or files to other devices.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils' Use of Personal Devices

- If a pupil breaches the school's e-safety policy regarding personal devices then the phone or device will be confiscated by a member of staff and will be held in a secure place in one of the the Vice Principals' offices. Personal devices will be released to the student in accordance with the school policy. If a potential criminal offence is suspected, the PSNI may need to be contacted.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone in the main office. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed (through the ICT curriculum) in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children or young people.
- Staff should use the school's phone switchboard where contact with pupils or parents/carers is required.

- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices should not be used during teaching periods unless permission has been given by a member of Senior Management in emergency circumstances.
- If members of staff have an educational reason to allow children to use a school issued device as part of an educational activity, then it will only take place when approved by Senior Management.
- **This guidance is a means of protecting both staff and pupils against unwarranted allegations**

School Website

- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Any material used by the school will be in keeping with the school's Child Protection Policy.
- Personal pupil information including home address and contact details will be omitted from school web pages**.**

Learning Platforms

An effective learning platform or learning environment can offer the school a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

The Learning Platform/Environment is subject to careful monitoring by the ICT Director.

- ICT Director and staff will regularly monitor the usage of the LP by pupils in all areas, in particular message, communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

Any concerns about content on the LP may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP for the user may be suspended.
- A pupil's parent/carer may be informed and appropriate outside agencies contacted.

Video Conferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures. The following guidelines must be adhered to when using the video conferencing facilities within school:

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the C2K broadband network should use the recommended conferencing software available in LNI
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.

Users

- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.

Content

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate to the class.

E-safety incidents of concern

- Parents will be asked to read the E-Safety Policy for pupil access and discuss it with their child, where appropriate.
- All students will return a parental signed copy of the E-Safety policy to the school.
- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- All incidents and actions concerning E-Safety will be recorded.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Sanctions

- Misuse of the Internet/electronic resources or thereby damaging the school's good name may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school will report any illegal activities to the appropriate authorities.

Please review the attached school Internet Acceptable Use Policy, sign and return this permission form to your son's Form Teacher.

Name of Pupil: _____

Form: _____

Pupil

I agree to follow the school's E-Safety Policy on the use of Internet. I will use the Internet and other electronic devices in a responsible way and obey all the rules explained to me by the school.

Pupil's Signature: _____

Date: _____ /_____ /_____

Parent/ Guardian

As the parent or legal guardian of the above pupil, I have read the E-Safety Policy and grant permission for my son or the child in my care to access the Internet. I understand that every reasonable precaution has been taken by the school to provide for online safety but they cannot be held responsible if pupils access unsuitable websites.

I accept the above paragraph ☐ I do not accept the above paragraph ☐
(*Please tick as appropriate***)**

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing children's work on the school website.

I accept the above paragraph ☐ I do not accept the above paragraph ☐
(*Please tick as appropriate***)**

Signature: _____

Date: _____ /_____ /_____

Dear Parent / Guardian

Re: E-Safety Policy

As part of the school's education programme we offer pupils supervised access to the Internet and other electronic resources. This allows students access to a large array of online educational resources that we believe can greatly enhance students' learning experiences.

However, access to and use of the Internet requires responsibility on the part of the user and the school. These responsibilities are outlined in the school's E-Safety Policy (enclosed). It is important that this enclosed document is read carefully, signed by a parent or guardian and returned to the school.

Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access inappropriate or objectionable material.

The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the E-Safety Policy.

Having read the terms of our school's E-Safety Policy, you may like to take a moment and consider how the internet is used in your own home, and see if there is any way you could make it safer for your own family. Useful information, to this end, can be obtained on a number of websites including the following:
www.ceop.police.uk
www.nspcc.org.uk

Yours faithfully

Mr D Clarke