St. Patrick's College, Banbridge

E SAFETY ACCEPTABLE USE POLICY

2019

Date ratified by Board of Governors: Michael Quinn

Signed by Principal: Robin Wood

Date of Review: **September 2019**

Date of next Review: **September 2021**

E-Safety and ICT Acceptable Use Policy 2019

1. Introduction

Our E-safety and ICT Acceptable Use Policy (AUP) has been written by the school, in the light of the Department of Education Northern Ireland (DENI) policy, and government guidance. It has been agreed by the staff and senior management team and approved by governors. It will be reviewed annually.

Use of the school's ICT equipment by all staff and pupils[1] must be in accordance with this policy. Any infringements of this policy will be treated in accordance with the sanctions in the Internet policy.

2. The Importance of Internet use in Education

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

3. Using the Internet to Enhance Learning

- The school Internet access will be designed expressly for staff and students use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

4. The need for pupils to learn to evaluate online content.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Co-ordinator who will report the URL to C2K.
- The school should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. The school will inform all staff and pupils of the appropriate way to use copyright material legally in school.

[1] *These include all teaching staff, support staff and technicians, substitute teachers, trainee / work experience teachers, language assistants, other visiting adults and pupils*

5. The Management of School e-mail.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

6. Management of the School Website Content

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Parents are asked for written permission from before photographs or video of pupils are published on the school Website at the beginning of the school year.

7. The Management of Newsgroups, Discussion Forums and E-mail Lists.

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- The use of video conferencing facilities in school will be for approved activities and all such use by groups of pupils will be monitored by staff members.
- Pupils will be allowed to take part in discussion forums that are controlled by staff or other responsible adults within and outside school using approved online learning environments, e.g. the school's VLE.

8. External Access to user areas and Learning Environments

- The school will grant select pupils and staff access to their user areas or VLE from home using their own username and password.

- The school is not liable for any loss or damage to pupils or staffs files caused unintentionally or by inappropriate or misguided use of the facilities.

9. The Management of Chat Rooms

- Chat rooms are not allowed to be used in school unless they are required for a specific subject for a specific purpose. When used they will be fully monitored by members of staff. The importance of chat room safety will be emphasised by staff prior to use.

10. Management of Emerging Internet Applications

- The policy on emerging technologies will be reviewed on an annual basis to take account of the risks associated with them.
- Mobile phones will not be used without permission during the school day between the hours of 8:45am and 3:15pm. This includes the use of any mobile technology to access the Internet or World Wide Web through the schools network or the public telecommunications network.
- Portable storage devices such as MP3 players, PDAs, Camera phones, or any other device that is capable of storing and displaying images or video, should also not be used between the hours stated above. However, the use of portable storage devices for transporting files between school and home is permitted under certain circumstances.
- Pupils and staff are allowed to use portable storage devices such as flash drives or memory sticks. However these must be checked prior to use for viruses.
- Neither pupils nor staff will be allowed to install applications of any type from portable storage devices without expressing permission of the ICT coordinator.
- Pupils and staff will only be allowed to use laptops or PDA's within the school if they can be checked by ICT staff for appropriate virus protection software or for the presence of unsuitable material.

- Pupils and staff will not be allowed to use such devices to access the Internet within school unless expressly permitted by a member of the ICT Coordinator or Principal.

11. The Management of Internet Access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.
- Parents will be informed that pupils will be provided Internet access
- Pupils must apply for Internet access individually by agreeing to abide by the Internet Usage Policy.
- Parents will be asked to sign the Internet policy in their homework diaries.

12. The Management of Risk Assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

13. The Management of Content Filtering

- The school will work in partnership with parents; C2K and DENI to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Coordinator.

14. Informing Students about the E-Safety and Acceptable use Policy.

- Rules for acceptable use will be found in their homework diaries.
- Students will be informed that Internet use will be monitored.

- Instruction in responsible and safe use should precede Internet access.
- Access to the use of ICT requires parental permission and a signed declaration by pupils agreeing to the school rules for use of ICT

- ICT is provided to enhance teaching and learning and provide means of communication between staff / pupils. While the use of information and communication technologies is an integral aspect of the Curriculum in St Patrick's College, access to ICT in St.Patrick's is conditional on pupils acting in a considerate and responsible manner. Access shall be withdrawn if a student fails to maintain acceptable standards of use, according to the conditions set out in this policy and general good practice.

- During school hours teachers will guide pupils towards appropriate materials. Pupils will always be supervised by a member of staff while using ICT facilities. However, it is at all times the pupil's responsibility to ensure that only appropriate material is accessed. The responsibility for monitoring the use of digital media and access to the internet at home lies with those with parental responsibility.
  St. Patrick's College will work constructively with parents / guardians to ensure that best practice is followed at all times.

- When using ICT at St. Patrick's College, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws or other statutory obligations.

14 B.SANCTIONS

- Disciplinary action will be taken in line with existing school rules and in line with the conditions set out in this policy.

- The extent of the sanction applied will depend on the nature and severity of the incident and will be applied in conjunction with the implementation of the school Discipline Policy.
  Violation of the above rules shall result in either a temporary or permanent ban use of either (a) the C2k network , (b) the internet or (c) both.

  - temporary (1 / 2 weeks, 1 month, 1 term, etc.)
  - permanent (until the end of the academic year)

- Parents/guardians shall be informed of serious breaches of the rules as laid out in this policy.

- In cases of serious misconduct, the school will inform the relevant authorities.

- Serious or persistent misuse of ICT equipment may result in the Board of Governors considering serious sanctions in line with the school discipline policy.

15. Staff Consultation.

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, learning managers, learning mentors, year heads, supply staff, classroom assistants, administration and caretaking staff, and Governors will be provided with the School Internet Policy, and its importance explained.

16. Maintaining the ICT System Security.

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.

- Security strategies will be discussed with C2K, particularly in regards to the Wide Area Network.
- If a member of the technical support staff leaves then all administrator level usernames and passwords will be changed.

17. The Management of Complaints Regarding the Internet.

- Responsibility for handling incidents will be delegated to the ICT coordinator.
- Any complaint about staff misuse must be referred to the Principal.

18. Enlisting Parental Support.

- Parents' attention will be drawn to the School Internet Policy in on the school Web site and pupil diaries.

19. Social Networking Sites

- The school will aim to educate parents and pupils of the dangers associated with social networking sites by offering support through the delivery of the curriculum.
- The school will investigate and take very seriously incidents of online bullying of pupils by pupils through social networking sites or via mobile phones when brought to our attention by staff, parents or pupils.
- If the school feels that a pupil has brought its reputation into disrepute by publishing unsuitable comments or images about other pupils or members of staff, or through publishing unsuitable materials that may appear to be linked to the school or identify the school in any unfavourable way then these matters will be investigated and suitable sanctions imposed. In extreme cases the social networking site in question, or the police, will be contacted to have the material in question removed.
- In such cases were the pupil is found to have broken the schools code of conduct, this will be considered serious misconduct and will be dealt with appropriately which may lead to suspension or expulsion.

Pupils are provided with preventative education with regards to keeping themselves safe on the Internet.