St. Patrick's Catholic Primary School E-Safety Policy

In the ever changing world we live in, technology is expanding and being used in many different and exciting ways, helping us expand our horizons. New technology is being released all the time letting us access information online and communicate with a whole world of new and exciting people. Each day we interface with many different forms of technology with the ability to connect and store personal information about us online. This doesn't necessarily mean that we are safe online!

We believe that:
Every child has the right to privacy. The law should protect the child's private, family and home life, including protecting children from unlawful attacks that harm their reputation.
Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.
Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.
(Articles 16, 17 & 19: UN Convention on the Rights of the Child)

This policy outlines the processes and guidance in place at St. Patrick's Catholic Primary School which safeguard and promote the well being of our staff and the students in our care.

Roles and Responsibilities

1. Directors

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors / Directors Sub Committee receiving regular information about e-safety. A member of the Board of Directors has taken on the role of E-Safety Director. The role of the E-Safety Director will include:

- meetings with the E-Safety Committee
- regular updates on e-safety incident logs
- regular updates on filtering / change control logs
- reporting to relevant Directors committee / meeting

2. The Headteacher and Leadership Group

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the college community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator (Miss L Barber).

- The E-Safety Coordinator and other relevant staff should receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / LG will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Mrs H Butters (Deputy Headteacher) is the CPO and a member of the E-Safety Committee. Miss L Barber (Assistant Headteacher) will supervise policy implementation.
- The Senior Leadership Team / LG will receive regular monitoring reports from the E-Safety Co-ordinator as will the ICT and E-safety Committee.
- The Headteacher and LG are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see Responding to Incidents of Misuse Policy" and relevant Local Authority HR / disciplinary procedures)

3. E-Safety Co-Ordinator (Miss L Barber)

The e-safety Co-ordinator is a member of the Leadership group. Their responsibilities include:

- leading the e-safety committee
- taking day to day responsibility for e-safety issues and having a leading role in establishing and reviewing the college e-safety policies / documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- providing training and advice for staff
- liaising with the Local Authority
- liaising with college ICT technical staff
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- meeting regularly with the E-Safety Director to discuss current issues, review incident logs and filtering / change control logs
- attending relevant meetings
- reporting regularly to Leadership group
- promoting and developing an E-safety conscious community

4. ICT System Officer (Mrs C Williams)

The Systems Officer is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Filtering software is kept up to date. We currently categorise subjects into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied. We are able to control our own permissions and add/amend to the defaults.
- the school's filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see "Internet Filtering Policy")
- that he keeps up to date with e-safety technical information in order to effectively carry out his e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in college policies

5. Teaching and Support staff

Teaching 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 college Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader / Class teacher as appropriate for investigation / action / sanction
- 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 / pupils 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, extra-curricular and extended school activities
- 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 college policies with regard to these devices

- In lessons where internet use is pre-planned students / pupils 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

6. Designated Safeguarding Lead (Mrs H Butters and Deputy DSL Miss L Barber)

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials including material of a sexual nature and/or material that aims to radicalise young people.
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

7. ICT and E-Safety Committee

Members of the ICT and E-safety committee will assist the E-Safety Coordinator with:

- The production / review / monitoring of the college e-safety policy / documents.
- The production / review / monitoring of the college filtering policy and Response to Incidents Policy
- Promotes and develops an e-safety conscious community

8. Students

Students:

- are responsible for using the college ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College systems.
- 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 college 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.
- Understand that bullying in any form is not tolerated and will be dealt with immediately. This is particularly true if a student is found to be an on-line bully.
- Know how to use social media safely and responsibly. Understand that once information / images are posted and shared it is very difficult to get them removed.
- 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 as well
- will be made aware that the school will investigate incidents occurring outside of normal school time and take action where appropriate
- such incidents will be recorded in the e-safety incidents database along with incidents occurring during normal school time.

9. Parents / Persons with Parental Responsibility

Parents / Persons with Parental Responsibility play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy

- accessing the college website / VLE / on-line student / pupil records in accordance with the relevant Acceptable Use Policy.

10. Community Users

Community Users who access school ICT systems / website / VLE as part of the extended school provision will be expected to sign a Community User AUP, before being provided with access to school systems

11. The Power to Discipline Beyond the School Gates

St. Patrick's takes seriously any bad behaviour which takes place beyond the college gates and students understand that they may be subject to sanctions where necessary and where lawful. This is particularly true where the behaviour:

a) Results in offsite bullying including through the use of mobile devices

b) Results in repercussions for the orderly running of the school

c) Poses a threat to another student or member of the public

d) Adversely affects the reputation of the school

e) Poses a threat linked to radicalisation

In all of these circumstances the Headteacher will consider whether it is appropriate to notify the police or anti-social behaviour co-ordinator in the local authority of the actions taken against a pupil. If the behaviour is criminal or poses a serious threat to a member of the public, the police will always be informed.

Policy Details

The School accepts its responsibility and commitment to take action over school related e-safety incidents that take place out of school. The school recognises the needs of young people at different ages and stages within the school and it will ensure that systems, teaching and learning, resources etc is differentiated to meet the needs of young people at different ages and stages within the school.

1. We have a nominated E-safety Co-ordinator (Miss L Barber).
2. The Director nominated for responsibility for E-Safety is Miss R Craven.
3. We carry out an E-Safety audit annually.
4. We have robust Acceptable Use Policies and all users sign up to them before they are allowed access to our systems.
5. We include e-safety measures in our SEF.
6. We keep an incident log and monitor our measures taken. This forms part of our whole school security database.
7. Cyberbullying is included in the school's anti-bullying policy.
8. Assemblies on e-safety are held annually and it is ensured that the content is age appropriate.

9. Students are introduced to the SMART rules during acts of worship, and they are reinforced in their ICT lessons.

10. The dangers of radicalisation and glorification of violence is discussed with student. Research concludes that children can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt these extremist views, and in viewing this shocking and extreme content may become normalised to it. The importance of recognising biased and misleading information is taught during discrete ICT lessons and reinforced across the curriculum whenever students use the World Wide Web. Robust filtering protocols drastically reduce the chances of students being exposed to this information in school.

11. Each student is provided with an e-safety leaflet.

12. Students all watch a Childnet approved video on cyberbullying.

13. All students take Computing in all year groups.

14. E-safety is delivered across the curriculum and mapped accordingly.

15. There are posters around the school that advertise methods of keeping safe on the Internet.

16. Students know how to report any concerns they may have.

17. All students have access to an online ICT / computing handbook which contains information on E-safety, password protection and Internet filtering procedures, advice on protecting personnel data and safe use of the college network, and the Internet.

18. All staff have access to an online ICT handbook which contains information on E-safety, password protection and Internet filtering procedures, advice on protecting personnel data and safe use of the college network, and the Internet.

19. All staff sign an AUP and new staff undergo ICT induction training.

20. All staff have received separate information on issues relating to e-safety.

21. The school's web site has a set of pages dedicated to e-safety. The pages contain guidance as well as links to policies, resources and other useful web sites. Updates to these pages are promoted to staff, pupils and parents. The school sends out information to parents when new updates are needed.

22. There are agreed procedures in school for the escalation of all issues of concern.

23. Staff portable electronic devices such as laptops and i-pads are returned annually to ICT Support team for internal checks which include safeguarding checks.

24. Each parent/guardian is provided with a leaflet about e-safety issues. The school web site has a dedicated set of pages about e-safety. Directors are provided with the same information and they approve the school's ICT security policy.

25. E-safety parent information evenings take place during the academic year.

26. The school seeks parental opinion on a number of issues on a regular basis which include e-safety. The results help us to decide on the information which is most needed by parents and Directors.

It is important that all of our staff are aware of the current legal requirements, national policies and guidance on the safeguarding and promotion of the well-being of children and young people. The measures outlined above

formulate a comprehensive college plan for keeping all parties safe. The statement below gives guidance on good practice and a list of do's and don'ts.

E-safety Statement

Students must be made aware of the dangers, both academic and real, of internet use, where relevant and pertinent to the topic being studied. Where lessons involve use of the Internet the following guidance should be adhered to:

1. 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.
2. 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.
3. It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the System Officer (Mr A Fox) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be made directly to Mr A Fox, with clear reasons for the need and the length of time that the filter change should remain in effect. Such requests are formally recorded.
4. 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
5. Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
6. As part of wider safeguarding responsibilities college staff should be alert to students accessing extremist material online, including through social networking sites.
7. 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.
8. Students should be made aware of the inherent dangers in irresponsible use of social media.
9. Staff are allowed to take digital / video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment / media; the personal equipment of staff should not be used for such purposes.
10. 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.
11. Students must not take, use, share, publish or distribute images of others without their permission
12. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
13. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
14. Written permission from parents or carers will be obtained before photographs of students are published on the school website (this is covered as part of the AUP signed by parents or carers at the start of their time at St. Patrick's). Student's work can only be published with the permission of the student and parents or carers. A list of students whose photo cannot be used is kept by the school administrator/ e-safety coordinator.
15. Staff should not accept "friend requests" from other members of staff without first checking the validity of the request.

Incidents

Where an e-safety incident occurs whether in or out of school it must be reported and recorded in the ICT Security database held by the E-Safety Co-ordinator and the actions outlined in the Response to Incidents Policy should be followed. Appropriate action must be taken forthwith and where necessary the Child Protection Officer informed.

Sanctions for Students

1. Failure to comply with any part of this policy will result in one or more of the following

    a. A ban, temporary or permanent, on the use of the internet facilities at school.

    b. A letter informing parents of the nature and breach of rules.

    c. Appropriate sanctions and restrictions placed on access to school facilities to be decided by the SLT/ E-safety Coordinator.

    d. Any other action decided by, E-safety Coordinator, Headteacher or Chair of Local Governing Board.

Supporting Documents

1. Internet Filtering Policy
2. Response to Incidents Policy
3. Use of Digital and Video Images Policy
4. Communications Policy
5. ICT Security Policy
6. Acceptable Use Agreements for staff and for students
7. Personnel Data Policy
8. Personnel Data Guidance
9. E-safety Audit.
10. E-safety Education at Painsley
11. Unsuitable web sites guidance
12. Staff ICT Handbook
13. Student ICT / Computing Handbook
14. College E-safety leaflet
15. College web pages on ICT security and E-safety.
16. College Safeguarding Policy

Reviewed November 2018