St Patrick's RC High School

A National Teaching School

On-line Safety
Acceptable Use Policy

Committee:	**Pupil Welfare**
Reviewed on:	**01.05.2019**
Reviewed by:	**Mr A Campbell**
Next Review:	**01.05.2020**

Signed: …….. **(Chair)**

St Patrick's RC High School

On-line Safety Acceptable Use Policy

School Mission Statement

"Our outstanding school community is guided by the gospel values, of love, forgiveness, reconciliation, justice, integrity, humility and truth faith and worship are lived, taught and celebrated. We recognise the importance of service to others and the opportunity to be witnesses to Christ in our community

All are unique and strive for personal growth. We celebrate the pursuit of academic excellence, applaud ambition and value the achievements of all. Our pupils are expected to achieve their best and use their learning to make a difference in the world they live in."

School British Values Statement

St Patrick's teachers uphold public trust in the profession and maintain high standards of ethics and behaviour. Teachers do this by not undermining fundamental British values and ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law.

Policy Status

Statutory

Rationale

This policy in accordance with the school mission statement reflects our active commitment to promote and safeguard the welfare of students and staff at our school. We believe that students and staff have a fundamental right to feel safe and protected from any form of abuse/exploitation via ICT systems and mobile technologies. Therefore, we aim to provide a secure, environment supported by a robust policy to promote safe practice and empower students and staff to protect themselves.

Our aim is to work with parents, but in the knowledge that children and young people have rights of their own, independent of their parents. Where there is conflict of interests between the parent/carer and the child, the school will operate in a professional manner, which serves the child's interests, re. The 1988 Children's Act. The rights of parents will be respected and the school will strive to ensure parents are informed of concerns raised by its staff with regard to on-line safety issues affecting their child/children.

The school has and will continue to develop a systematic approach towards-safety.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Roles and Responsibilities

Governors will:

Be responsible for the approval of the on-line Safety Policy and for reviewing the effectiveness of the policy.

The on-line safety Policy will be reviewed annually, in the light of any significant new developments in the use of the technologies, new threats to on-line safety or incidents that have taken place.

The Headteacher and Senior Leaders will:

Be responsible for ensuring members of the whole-school community are safe and adequately protected in relation to on-line safety procedures/issues in a school context.

Ensure that a member of the Senior Leadership Team is aware of the procedures to be followed in the event of a serious on-line safety allegation being made against a member of staff.

The On-line Safety Leader will:

- Ensure they attend regular and up-to-date training related to on-line safety
- Lead the on-line safety committee and/or cross-school initiative on on-line safety
- take day-to-day responsibility for on-line safety issues and have a leading role in establishing and reviewing the school on-line safety policies/documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an on-line safety incident taking place.
- Provide training and advice for staff.
- Receive reports of on-line safety incidents and create a log of incidents to inform future on-line safety developments.

Should serious on-line safety incidents take place, the following external persons/agencies will be informed:

- Chair of Governors.
- LA Safeguarding Officer and Director of Children's Services.
- Greater Manchester Police
- RM Education – ICT Managed Service Provider.
- Project Manager – Salford School Security – (Deborah Borg).
- iPad Technical Support – Mr D Shaw.
- Facebook.

The on-line safety Coordinator will also:

- Report to the Governors Pupil Welfare Committee on implementation/issues related to on-line safety at termly committee meetings.
- Report on the above to the Senior Leadership Team at regular intervals.

The Managed Service Provider and iPad Technician will:

- Ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the on-line safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority on-line safety Policy and guidance.
- That users may only access the school's networks through a properly enforced password protection policy.

Teaching and support staff will:

- Ensure they have an up to date awareness of on-line safety matters and of the current school on-line safety policy and practices.
- Ensure they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP).
- Ensure they report any suspected misuse or problem to the On-line Safety Officer and Safeguarding Officer for investigation/action/sanction These incidents will then be shared with the wider Senior Leadership Team and On-line safety Committee to inform future policy reviews.

The Designated Senior Leader for Child Protection will:

Ensure they attend regular training related to on-line 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.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Students will:

- Be responsible for using the school ICT systems and mobile technologies in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Endorsing (by signature) the Student Acceptable Use Policy Agreement (Homework Diary)

Parents/Carers

The school will take every opportunity to help parents understand these issues through Parent Forum meetings, parents' evenings, newsletters, letters, website and information about national/local on-line safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy Agreement (Homework Diary).
- Endorsing (by signature) the Use of Images Consent Form (Homework Diary)
- Accessing the school ICT systems and on-line resources e.g Mathswatch, MyEd, in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems and on-line resources e.g. RM Unify as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

On-line Safety Education and Training for Students

On-line Safety Education will be provided in the following ways:

A planned on-line safety programme will be provided as part of ICT lessons and the vertical tutoring programme of study. On-line safety will be regularly revisited in and will cover both the use of ICT and new technologies in and outside school.

- Key on-line safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students will 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.

Education and Training for Staff

All staff will receive on-line safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal on-line safety training will be made available to all staff.
- An audit of the on-line safety training needs of all staff will be carried out every 12 months.
- All new staff will receive on-line safety training as part of their induction programme, thus ensuring that they fully understand the school on-line safety policy and Acceptable Use Policies.

Education and Training – Parents and Governors

It is essential that Governors and parents receive on-line safety awareness and/or training and understand their responsibilities. Training will be offered as follows:

- A planned programme of on-line safety awareness/ training will be made available to Governors and parents.

Mobile Phones

Mobile phones may be brought into school. Students and staff may use them during break, lunchtime and after school.

Students and staff are not permitted to use them during lesson time unless permission has been given by the teacher for students to use apps in projects such as QR readers.

Permitted Communication Methods

Staff are permitted to use their personal phones/ipads/electronic devices to take photos/videos of pupils during lessons and activities for the purposes of the school website and social media (i.e. twitter). Once the photos have been uploaded they should then be deleted from the member of staff's personal phone, ipad or other electronic devices.

Forbidden Communication Activities

Staff must not capture, or store group/individual photos or videos of students or staff on personal phones or other camera devices, as part of an approved school activity without first seeking the consent of the individual, student/parent.

Staff are responsible for checking the list of pupils without photo/video permission from parents which will be stored in the staff shared area before any photos or videos are taken

Staff **MUST** delete all images/videos from personal devices, after upload to the school website/twitter account.

Staff must not use chat rooms, instant messages and social networking sites to communicate with pupils or parents.

Illegal Activities

The school believes that the activities referred to in the following section would be illegal and that users, should not engage in these activities in school or outside school or when using school equipment or systems.

- Child sexual abuse images.
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation.
- Adult material that potentially breaches the Obscene Publications Act in the UK.
- Criminally racist material in UK.
- Pornography.
- Promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Terrorism/radicalisation.

Where the school believes any illegal activities referred to above have taken place The school will take disciplinary action giving due regard to Safeguarding, Behaviour for Learning, Anti-bullying, Pupil Exclusion, Whistleblowing, Acceptable Use and Staff Disciplinary policies and the following external persons /agencies will be informed:

- LA Safeguarding Officer and Director of Children's Services.
- Greater Manchester Police.
- Chairman of Governors and Governors' Pupil Welfare Committee.
- RM Education – ICT Managed Service Provider.
- Project Manager – Salford School Security – (Deborah Borg).
- iPad Technical Support – Mr D Shaw.

Unacceptable Activities

The school will take disciplinary action in line with Safeguarding, Behaviour for Learning, Exclusion and Staff Disciplinary policies where of any member of the school community has:

- Used or passed on information which may be sensitive, offensive to other members of the school community or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Used school systems to run a private business.
- Used systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school.
- Uploaded, downloaded or transmitted commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealed or publicised confidential or proprietary information (e.g. financial personal information, databases, computer/network access codes and passwords).
- Created or propagated computer viruses or other harmful files.
- Carried out sustained or instantaneous high volume network traffic (downloading / uploading files) that caused network congestion and hindered others in their use of the internet.
- Used on-line gaming (non-educational) sites.
- Gambled – on-line.

- Accessed the internet for personal or social use (e.g. online shopping, banking etc) during lesson time.
- File shared e.g. music, films etc during lesson time.
- Used social non-educational networking sites during lesson time.
- Used of video broadcasts g e.g. YouTube (non-educational) during lesson time.
- Used external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses).

Restricted Activities

- Using school e-mail for personal use is forbidden (except for staff during break, lunch and after-school).
- Staff may access the internet for personal (e.g. on-line shopping) use during breaks, lunch before and after school.
- Use of You tube videos for showing to students (educational purposes) is permitted
- Educational on-line gaming may be used by students, on occasion, under the supervision of a member of staff.
- It is acceptable for staff to use the school website for blogs to communicate with pupils and to use on-line communities.
- Use of School Twitter accounts to communicate with pupils and on-line communities is also acceptable.

Further Information and Support

The UK Council for Child Internet Safety (UCCIS) www.education.gov.uk/ukccis

www.ceop.police.uk (The Child Exploitation and online Protection Centre)

R u cybersafe?

On-line safety tips about how to stay safe on-line:

http://www.salford.gov.uk/rucybersafe.htm

For online safety Practice Guidance for those who work with, volunteer with, and have a duty of Care to Safeguard Children and Young People:

http://www.salgord.gov.uk/d/e-Safety-Practice-Guidance.pdf

St Patrick's RC High School

Acceptable Use - Rules for Staff

To ensure that all adults within the school setting are aware of their responsibilities when using any ICT equipment and communications, such as the Internet or e-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

1. I know that I should only use the school equipment in an appropriate manner and for professional uses only.

2. I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via e-mail.

3. I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.

4. I have been provided with copies of the On-line Safety-Acceptable Use, Social Media and Photographs and Filmed Images of Children policies. I am aware that they are stored in the staff shared area. I have been advised to refer to them for guidance on school protocols so that I can communicate any problems that may arise, effectively and via the correct channels.

5. I know that taking, retaining and storing personal/individual photos/videos of students or staff on personal phones or other camera devices, as part of an approved school activity, without first seeking the consent of the individual, student/parent is forbidden.

6. I know that I must not store group/individual photos or videos of students or staff on my personal devices.

7. I know that I must delete photos/videos of students or staff from my personal devices immediately after upload to the school website or school twitter account.

8. I will report accidental misuse to the On-line Safety Leader

9. I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or On-line Safety Leader in accordance with procedures listed in the Acceptable Use Policy.

10. I know who the Designated Person for Child Protection is.

11. I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail.

12. I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or On-line Safety Leader.

13. I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

14. I will only install hardware that I have been given permission for.

15. I will not install software onto school equipment. I understand that this may only be carried out by the schools Network Manager.

16. I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password, I will check with the On-line Safety Leader.

17. I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves. I am aware that information relating to this act can be obtained from the On-line Safety Leader,

18. I will adhere to copyright and intellectual property rights.

I have read and understood the On-line Safety and Acceptable Use Policy in addition to the following associated policies:

- Photographs and Images of Children
- Social Media
- Data Protection
- Safeguarding
- Employee Code of Conduct

I agree with the above rules as I know that by following them I have a better understanding of on-line safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed……. Date…….

Name (printed)…….

Designated Lead For Child Protection	Mr M Connelly	**On-line Safety Leader**	Mr A Campbell

St Patrick's RC High School

Acceptable Use - Rules for Pupils and Parents

The school has installed computers with internet access to help your learning. These rules will keep you safe and help us to be fair to others:

- I will take responsibility for keeping myself and others safe on-line
- I will only access the system with my own login and password, which I will keep secret;
- I will not access other people's files;
- I will use the computers for school work and homework;
- I understand that using the computers to access inappropriate materials such as 'adult', racist or offensive material is forbidden;
- I will ensure that any external storage devices (such as USB Pen Drives) brought from outside school are checked to ensure they are virus free;
- I will ask permission from a member of staff before using the internet;
- I will only e-mail people I know, or my teacher has approved;
- I will only send messages that are polite and responsible;
- I will not take, store or share images of staff or other pupils without their permission;
- I will not give my home address or telephone number, or arrange to meet someone over the internet;
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I understand that if I do not follow these rules then I will have access withdrawn.
- I will seek help from a trusted adult if things go wrong.

As a user of the computer technology (including e-mail and the internet) provided by St Patrick's RC High School I agree to comply with the above rules for its use in a responsible way.

Pupil Name: ..... Form: .....

Pupil Signature: ..... Date: .....

As the parent or legal guardian of ..... I give permission for my son/daughter to use the computer technology (including e-mail and the internet) provided by St Patrick's RC High School. I understand that whilst the school has taken measures to provide a safe learning environment, pupils remain accountable for their own actions. I also understand that some materials on the internet may be objectionable (despite the filtering system), and I accept responsibility for setting standards for my son/daughter to follow when selecting and exploring information.

Parent/Guardian Signature: ..... Date: .....