St Richard Gwyn Catholic High School

E-Safety Policy September 2020

Policy Statement

Background

The School recognises that Information Technology, (IT) and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge students, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the School community. However, it is important that the use of IT and the internet is understood and that it is the responsibility of students, staff and parents, to use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Scope

E-safety does not just cover the Internet and available resources, but all different types of devices and platforms (e.g. Smartphones devices, wearable technology and other electronic communication technologies). The School understands that some adults and young people will use these technologies to harm children. The School has a ‘duty of care’ towards any staff, students or members of the wider school community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy governs all individuals who are given access to the school’s IT systems. This could include staff, governors and students however, sections of this policy may not be relevant to certain individuals due to their position, job role or subject to the age of the pupil.

Purpose

This policy aims to be an aid in regulating IT activity in School, and provide a good understanding of appropriate IT use that members of the School community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through the School’s anti-bullying policy and procedures.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures).

This policy is supplementary to the Pupil and Staff IT Acceptable Use (ITAUP) Policy but should also be read in conjunction with other material listed in appendix 1.

Mandate

Roles and responsibility

The Heads, Designated Safeguarding Leads, E-Welfare Leads and Governors will ensure that the e-safety policy is implemented and that compliance with the policy is monitored. The day-to-day management of e-safety in the School is the responsibility of the e-safety Lead. He / she will work closely with the Head of PSHEE and senior pastoral and academic staff in this regard.

The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of how students may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

Please read the Pupil / Staff IT Acceptable Use Policy for further information about the roles and responsibilities for e-safety within the School, including responsibilities for the security of the School's technical infrastructure and filtering systems.

Communicating School policy

All individuals issued access to the School's IT will be provided with a copy of the E-safety policy and this policy is available on the School website for all to access, when and as they wish. Extracts are also published in the IT Handbook. Rules relating to the School Code of Conduct when online, and e-safety guidelines, are displayed around the School and in all IT suites. E-safety is integrated into the curriculum in any circumstance where the internet or technology is being used, as well as being specifically addressed in the PSHEE curriculum. On joining the School, new and students and staff are required to agree to the Staff / Pupil IT Acceptable Use Policy. Existing staff may on occasion be required to re-sign this policy when significant changes are made.

Making use of IT and the Internet in School

Using IT and the internet in School brings many benefits to students, staff. The Internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a large part of everyday life, education and business. The School will endeavour to equip students with all the necessary IT skills for them to progress confidently between the key stages, into further education, or into a professional working environment once they leave Wellington.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students, (some age specific). 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 or device connected to the School network. The School cannot accept liability for the material accessed, or any consequences of internet access unless found to be negligent.

Expectations of use of School computers apply to staff and students both in and out of lessons.

Learning to evaluate internet content

With so much information available online, it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. “fake news”);
- to acknowledge the source of information used and to respect copyright. The School will take any intentional acts of plagiary very seriously, and as such, the School has a Copyright and Plagiarism Policy, which may be accessed on the School’s website;
- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

The School provides e-safety guidance to staff to better protect students and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

If staff or students discover unsuitable sites then the URL, time, date and content must be reported to the IT Department or any member of staff. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via the Director of IT or a member of the Senior Management Team. Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective.

Managing information systems

The School is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of School data and personal protection of the School community seriously. This means protecting the School network, (as far as is practicably possible), against viruses, hackers and other external security threats. The security of the School information systems and users will be reviewed regularly by the IT Support team and other third parties engaged with the School and led by the Director of IT. Anti-Virus and Malware protection software will be updated regularly. Some safeguards that the School takes to secure computer systems are:

- Making sure that unapproved software is not downloaded or installed to any School computers. Files held on the School network will be regularly checked for viruses;

- The use of user logins and passwords to access the School network will be enforced and unique.

- Portable media containing School data or programmes will not be taken off-site without specific permission from the Senior Management Team.

For more information on data protection in School, please refer to the School's Data Protection and information security Policy, which can be accessed on the School's website. More information on protecting personal data can be found in section 2.11 of this policy.

Emails

The School uses email internally for staff and students, and externally for contacting parents, and conducting day to day school business and is an essential part of School communication.

Access in School to external personal email accounts may be blocked. The School has the right to monitor emails, attachments and their contents but will only do so if there is suspicion of inappropriate use. The St Richard Gwyn Catholic High School Conduct for IT System Administrators policy gives the IT Team guidance and regulation in this area.

School email accounts and appropriate use

Staff should be aware of the following when using email in School:

- Staff should use their School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.

- Emails sent from School email accounts should be professional and carefully written. Staff are representing the School at all times and should take this into account when entering into any email communications.

- The School permits the incidental use of staff School email accounts to send personal emails if such use is kept to a minimum and takes place substantially out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the School nor should it include or refer to anything which may bring the School into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the School discovers that any member of staff has breached these requirements, disciplinary action may be taken.

- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their head of department or a senior member of staff.

- Staff must tell their head of department or a member of the Senior Management Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

- The forwarding of chain messages is not permitted in School.

- Further advice regarding email communication for staff is provided in the Staff IT Acceptable Use Policy.

The full protocol for staff use of the Internet and email is set out in the Staff IT Acceptable Use Policy

Students should be aware of the following when using email in School:

Students will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class:

- All students are provided with a School email account and students may only use approved email accounts on the School system during School hours.

- Students are warned not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases, will be restricted.

- Students should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

The full protocol for pupil use of the Internet and email is set out in the Pupil IT Acceptable Use Policy which students have to sign and can be found in student's diaries.

Published content and the School website

The School website is viewed as a useful tool for communicating School ethos and practice to the wider community. It is also a valuable resource for prospective parents and students, current parents, students and staff for keeping up-to-date with School news and events, celebrating whole-school achievements, personal achievements and promoting the School. .

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and transparency policies.

A team of staff, under the leadership of the HR Manager & PA to the Headteacher, are responsible for publishing and maintaining the content of the School website. The website will comply with the School's guidelines for publications including respect for intellectual property rights and copyright. Staff and students will be made aware of copyright in respect of material taken from the internet.

Staff and Students should take care not publish anything on the Internet that might bring the School into disrepute. Any pupil or member of staff is welcome to discuss material with the Director of Marketing, Deputy Heads or Heads.

Policy and guidance of safe use of children's photographs and work

Colour photographs and students' work bring the School to life, showcase students' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Images of students and staff will not be displayed in public, either in print or online, without consent, if the use of the image is considered by the School to be privacy intrusive. Whether consent is obtained from the parents or the pupil themselves will depend upon the maturity of the pupil. Please see the School's Transparency Notice for Students and Parents or more information about the use of photographs and videos.

Using photographs of individual children

Most people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, therefore the School has a Taking, storing and using images of Students Policy available on the School Website along with details of current consent forms.

Children may not be approached or photographed while in School or doing School activities without the School's permission, except for parents taking photographs or videos at School events involving their son or daughter for personal use only.

The School follows general rules on the use of photographs and videos of individual children:

- Consent will be obtained from either the parents or the pupil themselves (as appropriate) before using images in a way which is privacy intrusive. This may include images in: o School publications o on the School website o videos made by the School or in class for School projects.

- Electronic and paper images will be stored securely.

- Staff will only use equipment provided or authorised by the School, **(not their own device).**

- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (e.g. a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including in newspapers, full names will not be published alongside images of the child without the consent of the parents or the child (as appropriate). Groups may be referred to collectively by year group or form name.

- Events recorded by family members of the students such as School drama productions or sports events must be used for personal use only.

- Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

- Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification always, and will not have unsupervised access to the students.

- There is a list of all students whose photographs should not be published. This list is held in the staff shared area.

Complaints of misuse of photographs or video

Parents should follow standard School complaints procedure if they have a concern or complaint regarding the misuse of School photographs. Please refer to the Complaints Procedure for more information on the steps to take when raising a concern or making a complaint. Any issues or sanctions will be dealt with in line with this policy.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bullet-in boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that the School educates students so that they can make their own informed decisions and take responsibility for their conduct online. The School will normally block/filter access to social networking sites via the School network dependant on the age of the pupil. The School encourages parents with Children under the ages of 13 to follow the guidance of social media sites such as Facebook and not give their child access. Any such sites found by the School during their duty will be reported to parents and the website in question will be informed of the account and a request made for its removal.

Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are taught through the IT curriculum and PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place, (often referred to as a “digital tattoo”). The School follows general rules on the use of social media and social networking sites in School:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. Students are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School’s code of conduct regarding the use of IT technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Official School blogs created by staff or students / year groups /School clubs as part of the School curriculum will be moderated by a member of staff and must be registered only against a School controlled email account.

- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and students to remember that they are always representing the School and must act appropriately.

- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the Staff IT Acceptable Use Policy.

- Students and staff are not permitted to use “live streaming” features, (or equivalent) of social media platforms such as YouTube, Facebook, SnapChat or Instagram.

Mobile phones and personal mobile electronic devices (Smartphones), including wearable technology

Mobile phones and other personal devices are now an important part of everyone’s life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make students and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The School’s expectation is that mobile devices will be used responsibly at all times and certain measures are taken to ensure that staff and students adhere to this expectation. Staff / Students must follow the IT Acceptable Use Policy for further guidance on this matter.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the School.

Information about specific strategies to prevent and tackle bullying are set out in the School's Good Behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Any incidents of cyberbullying will be dealt with in accordance with the School's Promoting Good behaviour Policy and, where appropriate, the School's safeguarding and child protection policies and procedures.

Further information about cyberbullying is included in the Pupil and Staff IT Acceptable Use and Promoting Good Behaviour Policies.

Managing emerging technologies

Technology is progressing rapidly and innovative technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in School, and will consider any educational and pedagogical benefits that they might have. The School keeps up-to-date with modern technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting personal data

The School believes that protecting the privacy of staff, students, and parents and regulating their safety through data management, control and evaluation is vital to the whole school and individual progress. The School collects personal data from students, parents, and staff and processes it to:

- conduct day to day business processes (e.g. Finance, human resources etc.)
- support teaching and learning,
- monitor and report on pupil and teacher progress,
- strengthen pastoral provision.

The School takes responsibility for ensuring that any personal data that is collected and processed is used correctly and only as is necessary. We will keep parents fully informed of how personal data is collected, what is collected, and how it is used. Results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of personal data that the School processes. Please see the School's Transparency Notice for Students and Parents for more information and the School's Data Protection and Information Security Policy for further information. Through effective data management we monitor a range of School provisions and evaluate the wellbeing and academic progression of the School body, thus ensuring that we are doing all that is possible to support both staff and students.

In line with the General Data Protection Act 2018, and following principles of good practice when processing data, the School will:

- ensure that data is fairly and lawfully processed;
- process data only for limited purposes;
- ensure that all data processed is adequate, relevant and not excessive;
- ensure that data processed is accurate;
- not keep data longer than is necessary or legally required;
- process the data in accordance with the data subject's rights;
- ensure that data is secure;
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the School is required either by law or in the best interests of students or staff to pass information onto external authorities; for example, Disclosure & Barring Service (DBS), Independent School's Inspectorate, (ISI), Local Authority, Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the School's safeguards relating to data protection please read the School's Data Protection and Information Security Policy.