St. Patrick's High School

E-Safety, Acceptable Use of ICT & Social Media Policy

Latest Review: March 2021

Person Responsible: Mrs K McKenna

REVISED POLICY ADOPTED BY THE BOARD OF GOVERNORS

Signed:

Mission Statement

As a Catholic School in partnership with parents and the community, the school seeks to provide children of all abilities with a secure, caring, stimulating and happy environment where high values of work, personal integrity and learning can be achieved and where all pupils are encouraged to develop their talents and character and to contribute positively to home, school, church and society.

E-SAFETY, ACCEPTABLE USE OF ICT & SOCIAL MEDIA POLICY

This policy document contains policies in relation to use of the internet, use of mobile phones and use of digital/photographic images of children.

It has been developed within the context of current legislation, policy and guidelines including:

DENI Circular 2007/1 "Acceptable Use of the Internet and Digital Technologies in Schools"

DENI Circular 2011/22 "Internet Safety"

DENI Circular 2013/25 "e-Safety Guidance"

DENI Circular 2016/27 "Online Safety"

DENI Circular 2017/04 "Safeguarding and Child Protection in Schools – A Guide for Schools"

Education Authority (2020) "Guidance for Schools and EOTAS Centres Online Teaching Methods, Contact with Children and Families and Multidisciplinary Working"

DENI Circular 2020/5 - Guidance for Schools on Supporting Remote Learning

DENI: Pastoral Care in Schools (2001): Promoting Positive Behaviour

It should also be read in conjunction with the School's Safeguarding and Child Protection Policy; Anti-bullying Policy; Remote Learning Policy; Positive Behaviour for Learning Policy and Data Protection Policy.

CONTENTS

COVID ADDENDUM

COVID-19 ICT & E-safety

Policy addendum

Date: 03/03/2021 **Date shared with staff:**

Context

During the current school closures due to Covid-19 there has been an unprecedented and rapid change to the expectations around ICT usage to support remote home learning. As such this addendum covers the acceptable use of these new ways of working and will be integrated into an updated ICT & E-safety Policy in the future.

St Patrick's High School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Whilst staff are interacting with children away from school online, they must continue to adhere to the Staff Code of Conduct, ICT and E-Safety Policy and any other policies, protocols, professional standards and statutory guidance applicable to their role.

Phones

Staff should use parents' or carers' email addresses or phone numbers from management information system (SIMs). Use work accounts to communicate via email or online platforms, **never** u**se personal accounts**. All remote communication with students should be done exclusively via school approved IT platforms ie Google Classroom.

In light of our change in practice due to COVID19, it may be necessary for staff to use their personal mobile phones to communicate with parents and carers. Where this is deemed necessary, this must be agreed by a member of the Leadership Team. Where applicable, staff should make sure any **phone calls from a personal device are made from a blocked number,** so personal contact details are not visible. Keying 141 before the phone number will block your caller ID on the call you're making, or disabling it in settings.

Permitted Communication Methods

Staff are not permitted to use their personal phones/ipads/electronic devices to take photos/videos of pupils during lessons or activities.

Forbidden Communication Activities

Staff must not capture, share, or store group/individual photos or videos of students or staff on personal phones or other camera devices.

Children and young people are likely to spend more time online due to social distancing. Talk to them regularly about the benefits and risks of the online world and give them space to ask questions and talk about anything that worries them.

INTRODUCTION

St. Patrick's High School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice 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.

E-safety covers the internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. 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 aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT 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 pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our Positive Behaviour for Learning and Anti-bullying policy.

COMMUNICATING SCHOOL POLICY

This policy is available *from the school office and on the school website* for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during LLW lessons and assemblies where personal safety, responsibility, and/or development are being discussed.

GOOGLE CLASSROOM

St. Patrick's High School has chosen to use the Google Classroom suite as its main online platform for class based and remote student- teacher engagement in teaching and learning. Google Classroom compliments physical face to face teaching and learning in the classroom. Students have been allocated classrooms related to their various subjects and access codes to these classrooms. Online Classrooms are created, furnished and maintained by the appropriate subject teachers. As well as students in the class other staff members such as HoD will be invited to join these classrooms to support teaching and learning and to provide another layer of monitoring and protection for staff and students. It is hoped that Google Classroom will become an integral part of our school-based learning and therefore offer an easy transition when the school may be forced into unexpected closures due to Public Health and Safety guidance for example.

ROLES AND RESPONSIBILITY

ONLINE SAFETY AND RESPONDING TO A DISCLOSURE OR SAFEGUARDING CONCERN

The welfare and safety of pupils are the responsibility of **all** staff in school and any concern for a pupil's welfare MUST always be reported to the Designated Safeguarding Lead in accordance with the school's Safeguarding and Child Protection Policy.

ROLES AND KEY RESPONSIBILITIES

St Patrick's High School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The Senior Leadership Team will:

● Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
● Ensure there are appropriate and up-to-date policies regarding online safety, including acceptable use agreements for staff and pupils.
● Ensure that suitable and appropriate filtering and monitoring systems are in place.
● Work with technical staff to monitor the safety and security of school systems and networks.
● Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
● Support the Designated Teacher and Safeguarding Team by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
● Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
● Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
● Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Teacher / Safeguarding Team will:

● Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
● Keep up to date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
● Ensure all members of staff receive regular, up-to-date, and appropriate online safety training.
● Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
● Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches in liaison with the Head of ICT.
● Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
● Report online safety concerns, as appropriate, to the Senior Leadership Team and to Board of Governors through the Safeguarding Report.

● Work with the Senior Leadership Team to review and update online safety policies on a regular basis with appropriate stakeholder input.

The Creation of an Online Safety Committee:

The committee meets termly and consists of:

● The Designated Teacher responsible for Safeguarding
● Head of ICT
● Members of the iPad Group
● ICT Technical support

It is the responsibility of all members of staff to:

● Read and adhere to the online safety policy and to read, accept and adhere to the school's Staff Acceptable Use Agreement
● Take responsibility for the security of school systems and the data they use or have access to.
● Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
● Embed online safety education in curriculum delivery, wherever possible. Guidance and support should be appropriate to the age of the pupils.
● Have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care.
● Where pupils are allowed to freely search the internet during lessons, e.g. using search engines, staff should be vigilant in monitoring the content of the websites pupils visit and encourage them to use specific search terms to reduce the likelihood of coming across unsuitable material.
● Be aware of the potential for cyberbullying in their lessons where malicious messages can cause hurt and distress
● Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures as set out in the *Safeguarding and Child Protection Policy.*
● Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
● Take personal responsibility for professional development in this area.

It is the responsibility of staff managing the school technical environment to:

● Provide technical support and perspective to the Designated Safeguarding Lead and to the Senior Leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
● Implement appropriate security measures *(*including password policies and encryption*)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
● Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Senior Leadership Team and the Online Safety Committee.
● Report any attempts to disable or circumvent filtering and monitoring to the Designated Teacher and Senior Leadership Team, as well as to the school's technical support.
● Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the Designated Teacher, in accordance with the school's safeguarding procedures.

It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

● Engage in age-appropriate online safety education opportunities.
● Contribute to the development of online safety policies (through surveys and the Pupil Voice).
● Read and adhere to the school's Pupil Acceptable Use Agreement
● Respect the feelings and rights of others both on and offline.
● Take responsibility for keeping themselves and others safe online.
● Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

● Read the school's Pupil Acceptable Use Agreement and encourage their children to adhere to it and ensure they follow acceptable use rules at home.
● Discuss online safety issues with their children, reinforce appropriate, safe online behaviours at home and monitor their home use of ICT systems; (including mobile phones and games devices) and the internet.
● Role model safe and appropriate use of technology and social media.
● Identify changes in behaviour that could indicate that their child is at risk of harm online.
● Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
● Contribute to the development of the school online safety policies (through surveys and online safety events organised for parents/carers).
● Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

EDUCATION AND ENGAGEMENT APPROACHES

Education and engagement with pupils

- The school has established and embedded a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe, responsible and respectful internet use amongst pupils, including by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the Junior School Digital Literacy - Scheme of Work
- Enabling pupils to identify possible online risks and make informed decisions about how to act.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Teaching pupils how to recognise techniques used for persuasion or manipulation of others
- Ensuring pupils recognise acceptable and unacceptable online behaviour and know how and when to seek support
- The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:
- Reviewing the Acceptable Use Agreement during a Digital Literacy lesson before pupils signify their acceptance when they access the school network on a fixed computer.
- Displaying acceptable use posters in suitable locations around the school.
- Informing pupils that network and internet use will be monitored for safety and security purposes
- Rewarding positive use of technology by pupils.

Vulnerable Pupils

St. Patrick's High School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to Looked After Children and Previously Looked After Children, children with Special Educational Needs and Disabilities or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Our school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils and input will be sought from specialist staff as appropriate, including the SENCO.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with the school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues, or other members of the school community.

Awareness and engagement with parents and carers:

St Patrick's High School recognises that parents and carers have an essential role to play in enabling pupils to become safe and responsible users of the internet and associated technologies.

The school adopts a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This includes leaflets, local events and highlighting online safety at events such as parent evenings and transition events.
- Drawing their attention to the school online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information when their child joins our school
- Requiring them to read the pupil Acceptable Use Agreement and discuss its implications with their children.

REDUCING ONLINE RISKS AND SAFER USE OF TECHNOLOGY

St Patrick's High School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school device or other device connected to the school network. All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's Acceptable Use Agreements and highlighted through a variety of education and training approaches.

Classroom Use:

St. Patricks High School uses a wide range of technology. This includes access to:

- Computers, laptops, Chromebooks, iPad and other digital devices
- The Internet which may include search engines and relevant websites
- Google Classroom
- Email (web based)
- Webcams

All school owned devices (and personal devices used in school) will be used in accordance with the school's Acceptable Use Agreements and with appropriate safety and security measures in place.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our school community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Pupils will be appropriately supervised when using technology, according to their ability and understanding.
- Pupils will not be permitted to use their own personal devices to access the internet in class.

Managing Internet Access:

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an Acceptable Use Agreement before being given access to the school computer system, IT resources or internet.

Filtering and Monitoring

Decision Making

St. Patrick's High School ensure that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.

- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

The school works with **C2K** to ensure that our filtering policy and keyword detection is continually reviewed and updated. Lists of inappropriate websites are updated automatically by C2K and they block sites containing certain keywords.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Officer and/or the computer technicians.
- The breach will be recorded and the technical support will contact C2K who will add identified sites to the filtering policy.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies

Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:

- The school has a clear procedure for responding to concerns identified via monitoring approaches.
- These are reported to the Designated Safeguarding Officer in accordance with the Safeguarding and Child Protection Policy.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with GDPR.

Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly for PCs, administered centrally.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage or laptops) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be automatically checked by an anti-virus /malware scan upon use.
- The use of school accounts in the Google system to store school-related information
- The appropriate use of user logins and passwords to access the school network.

- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found in the Acceptable Use Agreements.

Password policy

All members of staff and pupils have their own unique username and private passwords to access school systems; members of staff and pupils are responsible for keeping their password private. We require all users to:

- Use strong passwords for access into our system.
- Always keep their passwords private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Managing the Safety of the School Website

- The school will ensure that information posted on our website is up to date and meets the requirements as identified by the Department for Education.
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- All administrator and editor accounts for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Publishing Images and Videos Online

The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): Data Protection Policy, Acceptable Use Agreements and the Staff Code of Conduct.

Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including Data Protection Policy, Acceptable Use Agreements, the Staff Code of Conduct.
- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked.
- Electronic communication which contains confidential information relating to identifiable pupils will only be sent externally using secure and encrypted email. Staff who are required to send sensitive data should be using pass worded documents
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Designated Safeguarding Officer if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

Staff

- The use of personal email addresses or personal social media accounts by staff for any official school business is not permitted.
- All members of staff are provided with a specific school email address, to use for all official communication.

Pupils

- Pupils will use school provided email accounts for educational purposes and for all use on school premises and for school purposes.

- All pupils will agree to an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

Management of Learning Platforms

St Patrick's High School uses Google Classroom as its official learning platform.

- Leaders and staff will regularly monitor the usage of the Google Classroom in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the Google Classroom.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled.
- Pupils and staff will be advised about acceptable conduct and use when using the Google Classroom.
- All users will be mindful of copyright and will only upload appropriate content onto the Google Classroom.

Any concerns about content on the Google Classroom will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the Google Classroom for the user may be suspended.
- The user will need to discuss the issues with a member of the senior leadership team before reinstatement.
- A pupil's parent/carer may be informed.
- If the content is considered to be illegal, then the school will respond in line with existing safeguarding and child protection procedures.
- A visitor may be invited onto the Google Classroom by a member of the leadership team; in this instance, there may be an agreed focus or a limited time slot.

SOCIAL MEDIA

The School defines social media as 'any websites and applications that enable users to create and share content or to participate in social networking'. Social networking sites and tools include, but are not limited to, Facebook, Twitter, Snapchat, Tok-tok, LinkedIn, MySpace, Flickr, YouTube and Instagram. It also includes forums and discussion boards such as Yahoo Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allows individual users or organisations to use simple publishing tools.

These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online.

Guidance for Students:

Students are taught through the ICT curriculum and LLW 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. The school follows general rules on the use of social media and social networking sites in school:

- The use of social media by pupils during school hours or with school devices is not permitted.

- Pupils are educated on the dangers of social networking sites and how to use them in a positive, safe, and responsible manner. They are all made fully aware of the school's code of conduct regarding the use of ICT and 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 password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils 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 pupils to remember that they are representing the school at all times and must act appropriately.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti bullying and behaviour. Concerns will be raised with parents and carers as appropriate, particularly when concerning underage use of social media sites and tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Example would include full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests, and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carers or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords that they do not share with anyone else.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.

Guidance for staff:

If staff are using social media to communicate with pupils, they must inform the E-safety Co-ordinator. Staff should only use the VLEs provided by C2k to communicate with pupils. (Currently Google Classroom, Blackboard Collaborate, Microsoft Teams and OneNote)

It is noted that the expectation that high quality learning and teaching can continue online during periods of exceptional school closure means that it may be essential for staff to communicate more regularly with pupils using online platforms. In such instances, the following should be considered:

- Online teaching is an extension of the classroom and should be covered by the school Acceptable Use Policy. All principles outlined by the Acceptable Use Policy will apply to all online teaching activity.
- Staff should avoid the use of personal mobile phones. In the exceptional circumstances where staff need to contact a parent/pupil by phone, this should be agreed by the principal or direct line manager.
- Staff should use only their school email accounts such as C2k and should avoid using personal accounts if contacting children or their parents.
- Staff should be aware that in the interaction with young people, all conventional professional teaching norms and standards will apply to online learning with children. Consider using camera-free conferencing, where the focus is on the content rather than the webcam images. Using the C2k platforms, teachers are able to maintain full control of the audio and video content and what is shared on the platform.
- Staff should not use personal social media accounts or personal text messages to contact pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Principal.

- It is advisable that staff do not have contact with past pupils. Staff may remain in communication with past pupils via a school email account or the school social media accounts.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Officer or Principal.
- Should staff have any concerns about what they see or hear online, this should be brought to the attention of the Safeguarding Team for the centre or Designated Teacher in School, in line with the school's Child Protection and Safeguarding Policy.
- Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Regard should be given to this Policy and related Policies, at all times both inside and outside of work.
- Members of staff must ensure that, wherever possible, and where the social media site allows, their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives or follow them on their personal accounts.
- Staff and volunteers must not engage in inappropriate use of social network sites which may bring themselves, the school, school community or employer into disrepute. Staff and volunteers should ensure that they adopt suitably high security settings on any personal profiles they may have.
- Staff should exercise caution in their use of all social media or any other web-based presence that they may have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others. This may also include the use of dating websites where staff could encounter students either with their own profile or acting covertly.
- Contact with students must be via school authorised mechanisms. At no time should personal telephone numbers, email addresses or communication routes via personal accounts on social media platforms be used to communicate with students. If contacted by a student by an inappropriate route, staff should report the contact to the Principal immediately.
- Photographs/stills or video footage of students should only be taken using school equipment for purposes authorised by the school. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be retained and destroyed in accordance with the schools Records Management Policy and Disposal Schedules.
- Staff must not publish photographs of pupils without written consent or parents/carers or the pupil themselves if they are deemed of the age and ability to provide their own consent. Standard practice is to publish only the first name and initial the surname unless permission has been given by parents or pupils deemed of the age and ability to provide their own consent) for the full name to be used.
- Staff must consider the Safeguarding Policy when making any posts on school social media accounts.