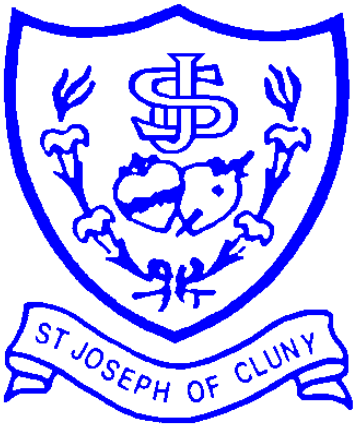

ST JOSEPH OF CLUNY

INTEGRATED ICT POLICIES

2013

Contents

Introduction

Social media, computer and mobile communication sites inclusive of chat rooms and networks such as Facebook are rapidly emerging forms of communication. This year has seen a huge increase in the media on the issue of cyber bullying and its impact on young people. There is no specific legislation governing Internet safety at school level and complicating this issue is the fact that the Internet functions in a global context whereas the law operates in a localised one. There are a number of legislations that have relevance to Internet safety including the Data Protection Act and its amendments but at the end of the day parents do play the primary role in protecting their children from the effects of the misuse of social media and internet sites and in protecting the wellbeing of other young people who are using these sites and ensuring the safety of all involved.

Cyber bullying is defined as the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm or humiliate others. It involves the abuse of another or causing damage to the reputation of another and circulating material recorded without consent to damage the reputation of another person. The effects may be deliberate or unintentional but the results are at a minimum hurtful and in the case of a significant number of young people can be devastating for them. Often it is difficult to prove and is sometimes hard to get other students to have the courage or understanding to report it.

Because of the instant and potentially permanent nature of access to material posted on social media and its capacity to multiply exponentially the new guidelines for schools are that a single inappropriate and offensive posting may constitute cyber bullying. Also the school, together with other relevant parties including parents/guardians, social media providers, Gardaí etc., has a responsibility – though not the sole one – for the promotion of the responsible use of social media and the prevention of their misuse.

When a student engages in inappropriate use of social media, even when not under the direct supervision of the school but where there is a clear connection with the school and there is a demonstrable impact on its aims, work reputation and /or personnel it is incumbent now on the school to intervene.

Developing and reviewing policies that relate to students' use of internet and social media requires that all linked policies have a consistent approach on the issue including the school Code of Behaviour and Discipline, the school Child Protection Policy and wider policies on Dignity in the Workplace etc. This Cyber bullying policy has been drawn up with the assistance of all partners including parents and students.

St Joseph of Cluny Computer and Internet Acceptable Use Policy (update 2013)

The aim of this Computer and Internet Acceptable Use Policy it to ensure that students will benefit from learning opportunities offered by the school's computer and Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school Computer and Internet Acceptable Use Policy is not adhered to this privilege may be withdrawn and appropriate sanctions imposed.

Before signing the permission slip, the Computer and Internet Acceptable Use Policy and the Cyber Bullying Policy should be read carefully so that the conditions of use are accepted and understood.

Acceptable Use

The computer system in this school has been established for a limited EDUCATIONAL PURPOSE. The term "educational purpose" includes classroom activities, career development and limited high-quality self-discovery activities such as project work and research.

The computer system has NOT been established as a public access service or a public forum. The school has the right to place reasonable restrictions on the material you access or post through the system. You are also expected to follow the rules set forth in your disciplinary code and the law in your use of the school computer system.

This Computer And Internet Acceptable Use Policy will be amended from time to time as is deemed necessary by the school. A copy will be made available to all new students. The current policy will be available to all the school. It is the student's responsibility to ensure familiarity with the current Computer And Internet Acceptable Use Policy**.**

Unacceptable Uses

The following uses of the school computer system are considered unacceptable:

1. **In the Interests of Personal Safety**
   You will not post personal contact information about yourself or other people. Personal contact information includes your address, telephone, school address, work address, photograph etc.

   You will not agree to meet with someone you have met online.

   You will not sign a 'guest book' on a web page on behalf of St. Joseph of Cluny Secondary School.

   You will promptly disclose to your teacher, to the IT Co-ordinator, to the Principal or to the Deputy Principal, any message you receive that is inappropriate or makes you feel uncomfortable.

2. **Illegal Activities**

You will not attempt to gain unauthorised access to the computer system or to any other computer system through the school computer system or go beyond your authorised access. This includes attempting to log on to another person's account or accessing, or interfering with another person's work or files.

You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. **These actions are illegal even if only for the purposes of browsing.**

You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

You will not use the computer system to engage in any other illegal act.

3. **System Security**

You are responsible for your individual account and should take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person.

4. **Commercial Use**

You may not use the computer system for commercial purposes. This means you may not offer, provide, or purchase products or services through the computer system.

5. **Inappropriate Language**

Restrictions in the use of inappropriate language apply to public messages, private messages and material posted on Web pages or on any computer in the school.

You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.

You will not post information that could cause damage, or danger, or disruption.

You will not engage in personal attacks, including prejudicial or discriminatory that could distress or annoy another person.

You will not knowingly or recklessly post false or defamatory information about a person or organisation.

6. **Respect of Privacy**

You will not re-post a message that was sent to you privately without permission of the person who sent you the message.

You will not post private information about another person.

You will not use your phone to take pictures in school without the permission of your teacher.

You will not post pictures or photographs of other people (inside or outside of school) without their permission.

7. Respecting Resource Limits

You will not install any Software Files without permission.

You will not use E-Mail without prior permission.

You will not use any form of messenger or 'Relay Chat'

You will not delete or rename existing Programs.

You will not download files, music, videos or games without permission.

You will not post chain letters or engage in 'spamming'. Spamming is sending an annoying or unnecessary message to a large number of people.

You will subscribe only to high-quality discussion group mail lists that are relevant to your education or career development.

You will not use any form of messenger or engage in any 'real-time' discussions, including 'Twitter' without permission.

8. Plagiarism and Copyright Infringement

You will not plagiarise works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours. All sources should be acknowledged.

You will respect the rights of copyright owners. Copyright infringements occur when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner.
You will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, one should follow the expressed requirements. In case of doubt permission should be sought from the copyright owner.

9. Inappropriate Access to Material

You will not use the computer system to access material that is profane or obscene (pornography) or that advocates illegal acts, or that advocates violence or discrimination towards other people.

If you mistakenly access inappropriate information, you should immediately tell your teacher, the IT Co-ordinator, the Principal or Deputy Principal. This will protect you against a claim that you have intentionally violated this policy.

Your parents/guardians should instruct you if there is additional material that they think it would be inappropriate for you to access.
The school fully expects that you will follow your parent's/guardian's instructions in this matter.

School's Strategy

The strategies employed by the school to maximise learning opportunities and reduce risks associated with the Internet will include:

- An IT acceptable use policy
- The operation of a comprehensive web filtering programme
- The school will regularly monitor students Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal USB keys or CD-ROMs or DVD's or downloading files from personal E-Mails in school requires a teacher's permission.
- Sanctions for not adhering to this policy will include:
    - Withdrawal of Computer privileges (Temporary or Permanent)
    - Demerits
    - Suspension

  Depending on the severity of the infraction

St Joseph of Cluny S.S. Cyber Bullying Policy 2013

Introduction

1. Social Media provide a dynamic and rapidly evolving means of communication. Mobile phones, chat rooms, websites and social networks, such as Facebook, play a significant role in many young people's lives as they interact with their peers and search for a social identity.
2. Inappropriate use of social media may lead to what is commonly known as Cyber Bullying.
3. Cyber Bullying is defined as the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm or humiliate another/others. It involves the abuse of another or causing damage to the reputation of another and circulating material recorded without consent to damage the reputation of another person.
4. It is an affront to human dignity and as such will be treated in accordance with the principles and procedures of this policy, the school Code of Discipline and Behaviour 2011, the school Policy on Anti-Bullying 2011, the Child Protection Policy 2012, the I.T. Acceptable Use Policy 2010, the school Health and Safety Statement 2012 and the school policy on Dignity in the Workplace.
5. Due to the instant, public, open and potentially permanent nature of access to material posted on social media and its capacity to multiply exponentially, a single inappropriate and offensive posting may constitute Cyber Bullying.
6. The school has a duty of care toward its pupils and its staff. A safe and respectful environment in school is necessary so that teaching and learning can take place.
7. The school acknowledges that parents are the primary educators and that it is primarily the responsibility of parents to guide and educate their children in relation to bullying and cyber bullying and their daughters use of mobile technology and social media.
8. The school has a responsibility along with the Gardai and other social media providers to promote the responsible use of social media and the prevention of their misuse, with special reference to Cyber Bullying.
9. This Cyber Bullying Policy applies even when a student engages in inappropriate use of social media, when not under the direct supervision of the school; when there is a clear connection with the school and/or a demonstrable impact on its aims, work reputation and/or personnel.

Definitions

Social Media Technologies are defined as information and communication technologies {ICT}, such as the internet, digital media or mobile phone which include text messages, group messaging services, instant messaging, personal websites, online personal polling websites, social media networks etc.

Cyber Bullying means any usage of Social media Technologies that seeks to undermine or humiliate a member, or members of the school community. This includes circulating or publishing through ICT, material recorded without consent for the purpose of undermining, or causing damage to, the professional or personal reputation of another person.

The instant and potentially permanent nature of access to material posted on social media and its capacity to multiply exponentially, means that a single inappropriate and offensive posting may constitute Cyber Bullying.

The Policy of the school

Cyber Bullying will be deemed a serious breach of the school's Code of Behaviour and Discipline and of the schools Anti-Bullying Policies. As such allegations of Cyber Bullying will be treated with the utmost seriousness by the school staff, Principal and Board of Management.

If the school becomes aware that a student is the writer of any messages, most particularly anonymous messages, that cause distress to our students or teachers which impacts on a person's self-esteem or their participation in the school, they will be subject to serious sanctions up to referral to the Board of Management.

Reporting Procedures

1. Any student or staff member who believes s/he has, or is being, subjected to Cyber Bullying, as well as any person who has reason to believe a student or staff member is being subjected to or has been subjected to Cyber Bullying shall immediately report the matter to the Year Head, Deputy Principal or Principal
2. All such reports will be investigated in line with agreed school procedures. Cyber Bullying will be subject to appropriate discipline and sanctions and may be referred to the Board of Management. The seriousness of the violation will determine the sanction to be applied by reference to the school Code of behaviour and Discipline.
3. Cyber Bullying may also be reported to the Gardaí or other outside agencies as appropriate.
4. False accusations by an individual of another student or member of the school community will also incur serious school sanctions.
5. Sanctions will be decided by the Principal and or the Board of Management and the seriousness of the violation will determine the sanction to be applied. This may range from positive behavioural interventions, up to and including suspension or expulsion. It should be further noted that Cyber Bullying using school technologies is in violation of the school's Acceptable Internet Use Policy.
6. Intervention techniques to prevent Cyber Bullying and to support and protect victims may include appropriate strategies and activities, as determined from time to time by the Board of Management and the Principal.

Appeals

Section 20 of the Education Act 1998 gives parents and students (aged 18 and over) the right to appeal certain decisions made by the Board of Management or by a person acting on behalf of the Board i.e. expulsions, cumulative suspension of 20 days, refusal to enrol. In general, appeals must be made within 42 calendar days from the date that the parents/guardians were notified of the decision.

Reprisal or Retaliation

The Board of Management will not tolerate reprisal or retaliation against any person who reports an act of Cyber Bullying. The consequence and appropriate remedial action for a person who engages in reprisal or retaliation shall be determined by the Board or Principal after consideration of the nature and circumstances of the act, in accordance with the principles of natural justice and Department of Education and Skills regulations and procedures.

The Principal and the Board of Management wish to encourage active reporting of all cases of Cyber Bullying and will support aggrieved persons throughout the process.

School Strategy

- The school maintains an IT acceptable use policy
- A school Code of Behaviour and Discipline that addresses bullying
- An annual school programme that addresses bullying issues from the school Tutor system, the SPHE programme and outside presenters including 'Sticks and Stones'
- Outside speakers i.e. this year a presentation from Child Watch Ireland on the subject of Cyber bullying was made to various Year groups, inclusive of the Parents Association
- The Pastoral Care programme
- A policy on cyber bullying as part of our computer and I.T. acceptable use policy
- Continuous review of our various care policies to ensure there is reference to internet safety
- Continuous dialogue with all partners including the Student Council, the Parents Association and the B.O.M on internet safety generally continuing the monitoring and filtering of internet sites in the school

Computer and Internet Use Permission Form

Please review the attached school Computer and Internet Acceptable Use Policy, sign and return this permission form to the Principal.

Student's Name:_____

Class:_____

Student

I agree to follow the school's Computer and Internet Acceptable Use Policy and Cyber Bullying Policy on the use of school computers and access to the Internet. I will use the computers and Internet in a responsible way and obey all the rules issued by the school. I understand that if I violate the rules I may face disciplinary measures. In the case of a breach of the Law, a criminal prosecution may result.

Student's Signature: _____ **Date:** _____

Parent/Guardian

As the Parent or legal guardian of the above student, I have read the Computer and Internet Acceptable Use Policy and Cyber Bullying Policy and grant permission for my daughter to use school computers and access the Internet. I understand that Internet access is designed for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites. I hereby release the School and its personnel from any and all claims and damages of any nature arising from my child's use of, or inability to use, the School computer system, including, but not limited to claims that may arise from the unauthorised use of the system to purchase products or services.

I will instruct my child regarding any restrictions against accessing material that are in addition to the restrictions set forth in the School Acceptable Use Policy and Cyber Bullying Policy. I will emphasise to my child the importance of following the rules for personal safety.

I give permission to issue an Account for my child and certify that the information contained in this form is correct.

Parent Signature: _____ **Date:** _____

Address: _____ **Telephone:**_____

_____

Occasionally, photographs or videos may be taken of students in the course of their school work or extra-curricular activities or competition winners etc. These may be used as teaching aids or be published on the School website or sent to local newspapers. **Parents will be contacted in advance of photographs being used to seek your permission for promotional use.** If you do not wish your daughter to have any promotional photographs of her, used by the school, please let the school know **in writing** by 30th September.

I understand and accept the terms of the Computer and Internet Acceptable Use Policy relating to publishing student's work on the school website.

Parent Signature: _____ **Date:** _____

What Parents Can Do

- Parents are the primary educators. It is parents' responsibility, not the school's to guide/educate their children in relation to bullying and cyber bullying.
- Parents/guardians must remain vigilant regarding their daughter's use of mobile technology and social media. In the same way as it is the duty of parents to advise their children against actions or comments that may be construed as a form of bullying, parents must advise and instruct on the dangers of cyber-bullying.
- First and foremost, we are asking that you dissuade your child from logging on to any site that allows anonymous postings. Such sites inevitably lead to trouble.
- Explore the parental advice posted on social media sites. Most of the advice is solid and reasonable.
- Agree sensible ground rules regarding the use of all social media including phones.
- Remind you child that no messages on-line or on texts or e-mails are entirely private. There are many examples of employees, colleges and others assessing applicants' presence on-line as part of application processes.
- Internet safety sites and links:

  www.esafety.ie – Internet safety

  http://www.internetsafety.ie/ - the Office for Internet Safety
  http://www.webwise.ie/ - Irish Government site
  http://www.wiredsafety.org - Parents
  http://www.netsmartz.org – Children
  http://www.digizen.org – Parents
  http://www.thinkuknow.co.uk - Good for working with your children
  http://www.reassureme.com – Internet protection and nanny net
  http://www.hotline.ie – reporting child pornography or abuse

  Also Facebook operate a help centre on their site – https://www.facebook.com/help/

Note:

While accepting that the use of social media is a feature of modern living, the school will show no tolerance, support or sympathy towards any users of social sites that allow anonymous postings. We ask our students, supported by their parents, not to log on to such sites (an example being 'ask.fm'). there are many, safer alternatives.

What Students Should Do

Everything that you put on-line or on texts is traceable back to you. You must show great care in what you write and in the type of photographs and other information that you post on social media sites. Ultimately there is sufficient technology to trace the writers of all postings including so called anonymous ones.

If the school becomes aware that you are the writer of any messages, most particularly anonymous messages, that cause distress to our students or teachers which impact on their self-esteem or their participation in school, you will be subject to serious sanctions up to referral to the Board of Management.

As well as showing great care in what you choose to text or to post on regular social media sites, we are asking you (with your parents' support) to not log on to any site that allow anonymous postings. By logging onto such sites you are exposing yourself to possible upset. The school cannot submit its limited resources investigating such matters that are easily avoided in the first place.

Cyber Bullying

If you receive unwelcome attention through social media or if you are experiencing any form of bullying, it is vital you do not suffer in silence. And if you witness bullying including cyber bullying, it is important that you take action and address the problem. The following is suggested:

- Never share private information on-line.
- Keep your passwords and pin numbers to yourself (except your parent). Do not share these with your friends.
- Do not reply to texts/messages that make your feel uncomfortable.
- Do not have any on-line conversation with people you do not know well.
- Save the evidence (photo/e-mail/video/web post, etc.) as proof, such as via 'print screen'.
- Tell your parent, a trusted adult, such as a close relative, a family friend, a teacher, health professional or a youth worker.
- Report the bullying to the Gardaí.
- Report the bullying to the technology providers such as the mobile phone company, web host or website owner.
- There are lots of useful sites on the internet advising you on internet safety, such as http://www.spunout.ie/health/Personal-safety/Internet-safety

Text Bullying

Texting is cheap, easy and can be great fun. Unfortunately it can also be used to harass, bully and frighten people. Text bullying or harassment can be texts that frighten, insult, threaten you or make you feel uncomfortable. E-mail, social networks like Facebook/Twitter and phone calls can be used to harass in the same way.

It is illegal to bully or harass someone by text, phone, Internet or E-mail and if the harassment is getting out of hand you should report it to the Gardaí.

If you are being bullied by texts:

- Don't stay quiet about the bullying. Tell a friend, your parents, a teacher or someone who will be able to help you and give you support.
- Don't respond and don't reply to the messages. If there's no answer, hopefully they will get bored and stop harassing you.
- Don't delete the messages; save a copy of whatever has made you feel uncomfortable. You can use them as evidence for reporting the crime.
- Report the bullying to the Gardaí and your phone company. They are aware of the problem and can give you a new phone number or caution the person harassing you.

Digital Fingerprint

Once something is posted online, be prepared to have it there **Forever.** If you wouldn't post it on a billboard in the city center, you shouldn't post it online. Be responsible about what you put on the internet now as it can have serious consequences in the future.

Social Networking Sites

'in order to be eligible to sign up for Facebook, users must be thirteen (13) years or older.' facebook.com

Remember that you don't know who your friend's friends are, and you don't know what they'll do with your picture or your phone number if you give it out by mistake.

Once your picture is out there, it's out there **forever** and you won't be able to get it back. Be aware that information on your profile could potentially be viewed by **anyone**.

Use your Privacy Settings. Adjust your account settings so only approved friends can instant message you. This means that people you don't want to see your profile can't

Photographs

The use of camera phones in school is not allowed without permission of the teacher in charge. You must always show great care regarding the photographs that you choose to place on-line. If you post any image of a student, teacher or employee of the school that has the effect of causing ridicule or distress, you will receive serious sanctions from the school.

Counselling

Any student who is upset by the matters raised in this note is free to meet with the School Counsellor, their Year Head or any teacher to discuss their concerns.

Remember – the basics

You're out in public – when online

Privacy features – giving you control.

Just because you can post anything **doesn't mean you should.**

The fact is you **shouldn't meet people in person who you only know from the Internet.**

Never, ever, agree to meet someone alone.

Staff Internet, E-Mail, and Computer Usage Policy (Update 2013)

The aim of this Computer and Internet Acceptable Use Policy it to ensure that staff can exploit and benefit from the school's computer and Internet resources in a safe and effective manner.

St Joseph of Cluny Secondary School provides computing resources and Internet access to members of the school staff for legitimate educational, academic and administrative purposes. All members of the school staff utilising Internet, E-mail and other computer resources are expected to be aware of specific policies governing their use. Specific usage policies and guidelines follow, but may not be all inclusive.

All policies are subject to change as the Internet/E-mail and computing network environment evolve.

This policy has been drawn up with reference to the following legislation;

- The Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act, 1998
- The Employment Equality Act, 1998
- The Non-Fatal Offenses against the Persons Act, 1995
- The Interception Act 1993
- The Data Protection Act 1988
- Video Recordings Act 1988

If the Staff Computer and Internet Acceptable Use Policy is not adhered to, access to the system will be denied and disciplinary action may be taken in accordance with the ASTI/JMB agreed disciplinary procedures. In addition, it should be noted that abuse of the Internet and other computer and electronic resources may become a matter of legislative jurisdiction above and beyond the question of professional ethics.

Policy Statement

The use of St Joseph of Cluny Secondary School (School) electronic resources, including computers, fax machines, and all forms of Internet/Intranet access, is for School business and for authorised purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (outside of normal school hours), and does not result in expense to the School. However, access to the computer systems for professional use must always be given priority.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the School's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of School computers, networks, and Internet access is a privilege granted by the School Management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate School purposes;

- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);

- Misrepresenting oneself or the School;

- Violating the laws and regulations relating to the use of electronic resources including the legislation referred to above.

- Engaging in unlawful or malicious activities;

- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the School's networks or systems or those of any other individual or entity;

- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;

- Sending, receiving, or accessing pornographic materials;

- Causing congestion, disruption, disablement, alteration, or impairment of School networks or systems;

- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;

- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;

- Defeating or attempting to defeat security restrictions on School systems and applications.

Using School automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory entity. Such material violates the School anti-harassment policies and is subject to disciplinary action.

The School's electronic mail system, Internet access, and computer systems must not be used to violate the laws and regulations of the state. Use of School resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

The School will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the School's automation systems is expressly forbidden.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files

The School owns the rights to all data and files in any computer, network, or other information system used in the School.

The School also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content.

Employees must be aware that the electronic mail messages sent and received using School equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by School officials at all times.

The School has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with this policy and legal requirements.

No member of staff may access another employee's computer files, or electronic mail messages without prior authorization from either the employee or an appropriate School official.

The School has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action.

Confidentiality of Electronic Mail

As noted above, electronic mail may be subject at all times to monitoring, and the release of specific information is subject to applicable legislation and School rules, policies, and procedures on confidentiality.

Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the staff notice board with your signature.

It is a violation of School policy for any member of staff, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others.

Policy Statement for Internet/Intranet Browser(s)

The Internet is to be used to further the School's mission, for educational and administrative purposes, and to support other direct job-related purposes.

The various modes of Internet/Intranet access are School resources and are provided as resources to staff members who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating School security policy, copyright, and licensing agreements.

All School policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, School information dissemination, standards of conduct, misuse of School resources, anti-harassment, and information and data security.

Guidelines for School Staff on using Social Media (JMB Bulletin 15)

Teachers are increasingly using the internet and social media sites as educational tools. It's important that teachers take precautions to safeguard themselves against cyber bullying and also protect their privacy. For example, connecting with students on social media sites can seem like and effective means of communication, however, this gives students potential to access personal information about teachers and the opportunity to target them with abusive behavior. The JMB Professional Behaviour Guidelines advocate:

"While it is appropriate to encourage and foster a warm friendly relationship with students, staff must always maintain and arms-length professional relationship. This arms-length relationship is equally applicable to in-school and out-of-school situations."

The Teaching Council Code of Professional Conduct for Teachers states:

"…ensure that any communication with pupils/students, colleagues, parents, school management and others is appropriate, including communication via electronic media, such as e-mail, texting and social networking sites"

These guidelines are equally applicable to online interactions between teacher and student as they are in the classroom.

With this in mind, please find below some practical consideration for school staff to safeguard themselves on social media sites:

Guidelines for Teachers

- Teachers should not use their personal Twitter or Facebook account for any school-related projects but should set up separate Twitter or Facebook accounts to use for school-related projects.
- Teachers should seek permission from school management to have access to the social media school –related projects they intend to run.
- Parents should also give permission for their child to participate.
- Use invitation-only discussion groups where possible. This means the teacher in charge of the project can control who joins and can moderate the content posted in the group.
- Avoid connecting directly with students by using Facebook 'pages' – in this case a student can access the page without having to be 'friends' with the teacher.
- School staff would be advised to maximize their privacy settings on Facebook for their personal profile. This will minimise the chances of students discovering a stall-member's personal profile. Privacy settings should also be adjusted appropriately for accounts used for school purposes. (see 'Optimise your Facebook privacy settings' in the useful links section for more information).
- Privacy settings do not guarantee absolute privacy as a 'friend' may pass on information.
- Teachers can 'protect' their tweets on Twitter. This means tweets are only viewable to approved users. This is good practice for personal and school-related Twitter accounts.
- Do not connect with people who cannot be identified or who post questionable content.

- Do not allow students to take pictures of school staff/students unless specifically required for a school project.
- School staff should avoid using personal photos in their profile information, or information about their job or school in their bio. Instead an icon or graphic and a non-school related bio could be used.
- School staff should not make any comments about students or post pictures of students using their personal profiles on social media sites.
- Check whether the school's Virtual Learning Environment (Moodle etc.) can be used as an alternative to public social media sites. The VLE is a school-mandated form of communication with students and less prone to abuse.

Useful Links

SPHE Bullying Prevention – First Steps for Teachers http://.sphe.ie/downloads/bull/bull_respond.pdf

The Stay Safe programme http://www.staysafe.ie

Secondary Assemblies for Online Safety http://optimums_education.com

Social Media glossary http://www.socialbrite.org/sharing-center/glossary

Webwise(NCTE program) http://webwise.ie

ThinkB4Uclick http://www.thinkb4uclick.ie

Optimise your Facebook privacy settings http://www.jmb.ie/component/content/article/428 (needs login)

Facebook page on Cyber-bullying

Twitter guidelines on Behaviour and Privacy and the Twitter Rules

Bully4u Anti bullying services: http://www.bully4u.ie

Cyber bully Info graphic/poster: Tell, Unfriend, Block,

Report: http://www.fuzion.ie/index.cfm/page/cyberbullying

How to report abuse on Facebook https://www.facebook.com/help/?faq=247013378662696

How to report abuse on Twitter https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/15789-how-to-report-violations#

Olweus Prevention Program http://www.violencepreventionworks.org