Saint Joseph's
CATHOLIC SCHOOL

Social Networking Policy (for staff & pupils)

Version 1.2 March 2022

ST JOSEPH'S CATHOLIC SCHOOL
CHURCH ROAD
LAVERSTOCK
SALISBURY
SP1 1QY

Success Criteria:		
Context/Aim: St Joseph's Catholic School creates and maintains a safe environment for all staff and pupils. All staff and pupils are protected from allegations and the school's reputation is safeguarded.		
Monitoring Procedures:		
By Whom: Governors' Academic Committee	**When:** Biennially	**How:** Report from Network Manager to Governors' Academic Committee Through the Safeguarding Annual Audit
Evaluation:		
By Whom: Head of ICT Faculty and Network Manager	**When:** Biennially	**How:** Report from Head of ICT & Network Manager to Governors' Academic Committee

Revision History:			
Version	**Approved and Ratified**	**Review Date**	**Additional Notes**
1.2	March 2022	March 2024	Updated sites/platforms in popular use
1.1	January 2017	January 2019	Addition to paragraph 'Social Networking as part of School Service'
1.0	July 2015	July 2016	Separated from E-Safety Policy

Vision Statement:

St Joseph's is a co-educational, 11-16 Catholic voluntary-aided school in the diocese of Clifton and the county of Wiltshire. Our aim is to provide a caring educational environment where each person is valued and is given the dignity due to a child of God.

At the heart of our school is the Christian vision of the human person. We want each member of our community to grow as an individual witness to the gospel values of love, truth, and justice. We want each pupil to be healthy in mind, body, and spirit.

Each member of our community should feel safe and secure in the learning environment. We aim to develop a sense of self-discipline and responsibility in our pupils. Everyone in our community should show respect for themselves, respect for others and respect for the environment.

We believe that each pupil should have the opportunity to enjoy and achieve to their full potential. We are committed to praising and celebrating achievement. We want our pupils to have high expectations of themselves to understand the value of service to others and our responsibility as stewards of the environment. Everyone has a contribution to make in helping to build the common good. We aim to equip our pupils with the ability to make good choices in their lives based on the positive relationships and values they have learned in St Joseph's.

We aim to help each of our pupils to develop morally and spiritually. We want them to achieve economic well-being while being mindful of the needs of others who are less fortunate.

We are committed to aspiring for excellence in all that we do for the sake of the Gospel.

Head teacher

National Policies and guidance/courses referred to and incorporated into SJCS Policy:	
Document/Course Title:	**Document/Course Date:**
Computer Misuse Act	1990
Data Protection Act	1998
Freedom of Information Act	2000
Communications Act	2003
Malicious Communications Act	1988
Regulation of Investigatory Powers Act	2000
Trade Marks Act	1994
Copyright, Designs and Patents Act	1988
Telecommunications Act	1994
Criminal Justice & Public Order Act	1994
Racial and Religious Hatred Act	2006
Protection from Harassment Act	1997
Protection of Children Act	1978
Sexual Offences Act	2003
Public Order Act	1986
Obscene Publications Act	1959 and 1964
Computer Misuse Act	1990
Data Protection Act	1998

Other SJCS Policies that relate to this Policy:
Child Protection Policy
Safeguarding Policy
Behaviour Policy
Whistleblowing Policy
Staff Code of Conduct
E-Safety Policy

Introduction to the Policy

St Joseph's Catholic school is fully aware and acknowledges that increasing numbers of adults and children are making use of social networking sites.

The widespread availability and use of social networking brings opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance aims to protect and inform staff and to help and advise on how to deal with potentially inappropriate use of social networking sites.

Purpose

The purpose of this policy is to ensure:

- That the school is not exposed to legal risks
- That the reputation of the school is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school

Objectives

The policy aims to:

- Assist staff to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Prevent adults abusing or misusing their position of trust

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Head teacher of the justification for any such action already taken or proposed. This policy should not be used to address issues where other policies and procedures exist to deal with them. It does not replace or take priority over advice given by Children's Services, the school's codes of conduct dealing with allegations of abuse, other policies issued around safeguarding children or IT issues, but is intended to both supplement and complement any such documents.

Scope

This policy applies to all adults who work at St Joseph's Catholic school. This includes teachers, support staff, supply staff, Governors, contractors and volunteers.

References to staff should be taken to apply to all the above groups of people. Reference to pupils means all pupils registered at the school.

For the purpose of this policy, 'social networking sites' is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Websites such as Facebook, Tik Tok, Snapchat, Instagram, and WhatsApp are perhaps the most well-known examples of social networking sites, but the term also covers other web-based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. In the post pandemic world, our use of Teams also falls into this category as do other educational services such as Seneca, Satchel One and other MFL platforms. This definition of social networking is not exhaustive as technology develops with new ways of communicating advancing every day.

All staff and pupils should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Use of Social Networking Sites in Work Time

Use of social networking applications in work time for personal use is not permitted unless permission has been given by the Head teacher.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party such as Twitter) must be approved by the Head teacher first. This should only be used for the purposes of, for example, advertising and communicating with parents. Photos of students should only be used when parents have agreed to this for advertising purposes.

Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head teacher. However, staff must still operate in line with the requirements set out within the policy.

Terms of Use

Staff must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all staff. This includes, but is not limited to, public facing applications such as open discussion forums, and internally facing uses such as project blogs regardless of whether they are hosted on the school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. St Joseph's Catholic school expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Social Networking applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual, or offensive nature that may bring the school into disrepute
- Must not be used for the promotion of personal financial interests, commercial ventures, or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put staff in breach of school codes of conduct or policies relating to staff
- Must not breach the school's misconduct, equal opportunities, or behaviour policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils, or parents
- No staff member should have a pupil or former pupil under the age of 16 as a 'friend' to share information with. Caution should also be taken before becoming 'friends' with ex-pupils who are over the age of 16 where siblings continue to attend the school
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent, or school activity / event unless prior permission has been obtained and agreed with the Head teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action
- Staff need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, could result in formal action being taken against them

Violation of this policy can be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/Protection for Staff on Using Social Networking

General

- No member of staff should interact with any pupil in the school on social networking sites
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 16

- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend
- Where family and friends have pupils in school and there are legitimate family links, please inform the Head teacher in writing
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils and staff interacting using social networking sites, please contact the named DSL in school

Personal Responsibility

- St Joseph's Catholic school staff are personally responsible for the content they publish online. Staff should be mindful that what they publish will be public for a long time. Once materials have been published online, they may be out of the control of the publisher
- Online behaviour should reflect the same standards of honesty, respect, and consideration that is used face–to–face and should be carried out consistent with the standards applied on school premises and in furtherance of the school's Catholic ethos
- When posting to a blog, discussion forum, or Twitter or Facebook account, staff must ensure that they make it clear that the information is representative of their views and opinions and not necessarily the views and opinions of St Joseph's Catholic School. Blogs, wikis, discussion groups, and podcasts can be seen as an extension of the classroom. What is inappropriate in the classroom should be deemed inappropriate online
- The lines between public and private, personal, and professional are blurred in the online world. By virtue of identifying themselves online as affiliated with St Joseph's Catholic School, staff are now connected to colleagues, pupils, parents, and the school community. Staff should therefore ensure that content associated with them is consistent with their work at the school
- Staff should not participate in spreading false or unsubstantiated rumours or false information
- Staff should strive to speak the truth – and when they don't know, sometimes saying nothing is the best choice
- When contributing online staff must not post confidential pupil information
- Before posting videos and photographs of pupils to any online forum, including Facebook, a blog or any other media, prior permission of the Head teacher must be obtained. Such a request should include the content of what you intend to post, where you intend to post it, and the identity of any St Joseph's Catholic School staff or pupils
- Such materials should ONLY be posted to social media that provides reasonable protection against general public access and has tools in place to limit access only to identified or invited persons

Disclaimers

- St Joseph's Catholic School staff must include disclaimers within their personal blogs and other media in which they either identify themselves or are likely to be identified as affiliated with the school that the views are their own and do not reflect on St Joseph's Catholic School. For example, "The postings on this site are my own and do not necessarily represent the positions, strategies, or opinions of St Joseph's Catholic School"

- Where online media is open to content and participation (such as comments) from pupils and parents, teachers are encouraged to carefully review and moderate such comments or disable their use

Guidance/Protection for Pupils on Using Social Networking

General

- No pupil may access social networking sites during the school working day
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens
- No school computers are to be used to access social networking sites at any time of day
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision
- Please report any improper contact or cyber bullying to the DSL or Safeguarding Team
- We have a zero tolerance to cyber bullying.

Protection of Personal Information

Adults working in schools should:

- Never share their work logins or passwords with other people
- Keep their personal phone numbers private
- Not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address should be used
- Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises
- Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people

Adults working in schools should not:

- Use school equipment for personal use, e.g. cameras
- Use their own mobile phones to contact pupils or parents

Communication Between Pupils / Adults Working in School

Communication between pupils and adults by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, webcams, websites, and blogs.

The school normally provides a work mobile and e-mail address for communication between staff and pupils where this is necessary for a particular trip. Adults should not give their personal mobile numbers or personal e-mail addresses to pupils or parents for these purposes.

Adults should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.
Adults should not give their personal contact details to pupils including e-mail, home, or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites.

Agreed protocols include the use of Teams, Office 365, School email system and Satchel One.

Child Protection Guidance

If the Head teacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above, they should:

- Record the disclosure in line with their Child Protection Policy. The school must refer the matter, also in line with the Child Protection Policy
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes
- If disclosure comes from a member of staff, try to maintain confidentiality
- The Governors and Head teacher, in consultation with the necessary Authorities, will advise whether the member of staff should be suspended pending investigation after contact with the Police. It is not recommended that action is taken until advice has been taken
- If disclosure is from a child, follow the normal process in the Child Protection Policy until the police investigation has been carried out

Cyber Bullying

By adopting the recommended no pupil use of social networking sites on school premises, St Joseph's Catholic school protects themselves from accusations of complicity in any cyber bullying through the provision of access.

Parents should be clearly aware of the school's policy of access to social networking sites. Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.

This can be a complex area, and these examples might help:

- *A child is receiving taunts on Facebook/Snapchat/Instagram/TikTok and text from an ex-pupil who moved three months ago: This is not a school responsibility, though the school will contact the parents to broker a resolution.*

- *A child is receiving taunts from peers. It is all at weekends using MSN and Facebook/Snapchat/Instagram/TikTok. The pupils are in the school: The school has a duty of care to inform the parents.*
- *A child is receiving taunts from peers. It is all at weekends using Facebook Snapchat/Instagram/TikTok. The pupils are in Year 7: This is the tricky one. The school has a duty of care to inform the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the school's recommendation. They could then deal with residual bullying in the school but refuse to deal with the social networking issues.*

Once disclosure is made, investigation will have to involve the families. This should be dealt with under the schools adopted behaviour policy.

If parent / carers refuse to engage and bullying continues, it can be referred to the social media platform and / or Police as harassment. This guidance can also apply to text and mobile phone cyber bullying.

Appendix (i)

School staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action, that is illegal if committed offline, is also illegal if committed online.

Computer Misuse Act 1990
This Act makes it an offence to:

- *Erase or amend data or programs without authority;*
- *Obtain unauthorised access to a computer;*
- *"Eavesdrop" on a computer;*
- *Make unauthorised use of computer time or facilities;*
- *Maliciously corrupt or erase data or programs;*
- *Deny access to authorised users.*

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- *Fairly and lawfully processed;*
- *Processed for limited purposes;*
- *Adequate, relevant and not excessive;*
- *Accurate;*
- *Not kept longer than necessary;*
- *Processed in accordance with the data subject's rights;*
- *Secure;*
- *Not transferred to other countries without adequate protection.*

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- *Establish the facts;*
- *Ascertain compliance with regulatory or self–regulatory practices or procedures;*
- *Demonstrate standards, which are or ought to be achieved by persons using the system;*
- *Investigate or detect unauthorised use of the communications system;*
- *Prevent or detect crime or in the interests of national security;*
- *Ensure the effective operation of the system.*
- *Monitoring but not recording is also permissible in order to:*
    - *Ascertain whether the communication is business or personal;*
    - *Protect or support help line staff;*
    - *The school reserves the right to monitor its systems and communications in line with its rights under this act.*

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non–commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: –

- *Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or*
- *Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.*

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Social Networking Policy

I hereby confirm that I have read and understood the attached Social Networking Policy and that I agree to abide by the requirements of the policy. Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Name:

Signed:

Date: