Saint Joseph's
CATHOLIC SCHOOL

Online Safety Policy

Version 3.0 – March 2025

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:	When:	How:
Governors' Academic Committee	Biennially	Report from Network Manager to Governors' Academic Committee / Through the Safeguarding Annual Audit

Evaluation:

By Whom:	When:	How:
Assistant Head, Safeguarding Team and Network Manager	Biennially	Report from Deputy Head / Assistant Head & Network Manager to Governors' Academic Committee

Revision History:

Version	Approved & Ratified	Review Date	Additional Notes
V 3.1	March 2025	March 2027	Full re-write to bring up to date with recent guidance. Re-named to Online Safety Policy.
V 2.2	March 2022	March 2024	Updated to reflect use of new platforms in school (Teams, Office 365 & Satchel One).
V 2.1	January 2017	January 2019	None
V 2.0	December 2015	December 2016	Total re-write
V 1.4	January 2014	January 2015	-
V 1.3	February 2013	November 2013	-
V 1.2	November 2011	November 2012	-
V 1.1	November 2010	November 2011	-

Vision Statement:

With God's love and inspiration, we aspire and achieve excellence.

Vision: St. Joseph's aspires to be an exceptional, inclusive Catholic school where every individual feels a **profound sense of belonging and recognises their spiritual gifts.** In a safe, trusting, and respectful environment, everyone can thrive.

The St Joseph's family is dedicated to providing and receiving **outstanding educational opportunities, enabling each member to achieve excellent progress and outcomes** in every aspect of school life to ensure the highest level of academic results. We are committed to nurturing God-given talents and encouraging everyone to reach their full potential, fostering spiritual and moral character development.

1. Introduction to the Policy

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schoolshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.4 The Network manager

The Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by e-mailing safeguarding@sjcs.org.uk and ithelpdesk@sjcs.org.uk
- Following the correct procedures by contacting the network manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects such as PSHE and other mediums such as assemblies, where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' information evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyberbullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The safeguarding team, Senior Leadership, Heads of Year, Classroom Teacher, Form Tutors and external speakers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher may carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from safeguarding team.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the safeguarding team and the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school behaviour policy and the searching / confiscation procedures laid out within it

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

St Joseph's recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St Joseph's will treat any use of AI to bully pupils very seriously, in line with our behaviour and anti-bullying policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

The school is currently developing an AI usage policy for staff and students.

7. Acceptable usage of the internet

All pupils and parents/carers sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices inside of school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons

- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Devices are expected to be stored safely and silently during the course of the school day (08:50-15:30).

The Headteacher may grant special exceptions for this in cases where mobile phones will be beneficial to the learning and progress of students in a specific class / task / subject.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the DSL and / or Network Manager.

The school will provide annual cyber security training for staff which will further educated them on online safety issues and around use of all their devices.

10. Responding to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

All staff will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The school employs high-level filtering and monitoring via Senso. All breaches are logged and regular reports of online activity are shared with the safeguarding team. Any acute breaches or concerns will be immediately reported to the school.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix (i) Pupil Acceptable Use Agreement

Network Usage Agreement

Acceptable use of the school's computer network, internet, and e-mail facilities.

This acceptable usage policy is designed to outline the rules for safe, responsible, ethical, and legal ICT use by pupils within St Joseph's Catholic School.

The computer system and all IT equipment is owned by the school and is provided to enhance learning. Any work or activity undertaken using school IT equipment must be directly related to learning. In order to maintain high levels of security the school reserves the right to regularly monitor and examine or delete any files which contain inappropriate material. Users are responsible for their own good behaviour. General school rules apply whilst using the computers.

Guidelines: using the computer network

- Pupils must be supervised by a member of staff at all times.
- Access should only be made via the authorised account and password, which must not be given to another person.
- No attempt should be made to move or repair any network device – this includes computers, printers, and all peripheral connections.
- Please report any problems or damage to the network manager or a member of staff.
- The introduction of any personal computers/laptops to the school network via a network point or our wireless system is not permitted.
- It is illegal to use the school IT facilities for personal financial gain, gambling, political purposes, or advertising.
- In order to comply with Health and Safety regulations, No food or drink to be consumed in the IT areas.
- At the end of the lesson please log off ready for the next user. Do not shut down the computer unless instructed to do so.

Our internet service provider monitors all internet use and administers a strict filtering policy encouraging effective use of the internet in school. A record is kept of every site visited via the school system, access to illegal sites will be reported to the police.

You should be aware that the network manager can view your computer screen from the school network without your knowledge, at any time.

Guidelines: using the internet

- All internet activity will be appropriate to school studies. Please do not waste time playing non educational games.
- Do not try to breach the SWGFL filter or deliberately access inappropriate material.
- For your own safety it is important that you do not give any personal information, ie your name, mobile phone number or home address via any internet site. You must not give information about any pupil or member of staff.
- Do not download music or any other software, you may be breaching copyright laws.
- Plagiarism is unacceptable and will result in loss of marks or disqualification from public examinations.
- E-mails should be written carefully and politely. E-mails designed to cause anxiety, irritate, inflame or promote argument should not be sent as they may be interpreted as bullying. Remember that sending abusive or threatening message is against the law.

If you feel you are being bullied by email, text or online tell a member of staff as soon as you can. Do not reply to any threatening or unpleasant messages.

Network Usage Agreement (continued)

Failure to abide by the guidelines as stated will be taken very seriously. Pupils abusing their internet privileges will be denied access for one week and an after-school detention will be imposed. In these cases, the pupils' access will only be reinstated once the detention has been served.

Pupil Commitment:

- I have read and understand this document.
- I agree to comply with the guidelines.
- I understand that failure to do so will result in my privileges being withdrawn.

Pupil Name:

.....

.....

Signed: ..... **Date:**

.....

Parent/Carer Statement:

- I recognise that whilst every effort will be made to monitor pupils' use of the internet it is impossible for St Joseph's School to monitor the use of the system continuously or to restrict access to all controversial material.
- I give my permission for my child to use the internet and e-mail where appropriate.
- I agree to reimburse the school should any cost be incurred as a result of my child's actions.

Parent/Carer name:

.....

Signed: ..... **Date:**

.....

Appendix (ii) Staff Acceptable Use Agreement

ST JOSEPH'S CATHOLIC SCHOOL

STAFF— Acceptable User Policy for the use of I T facilities.

Staff are expected to familiarise themselves with the contents of this Code and act in accordance with the principles set out in it. All staff with access to the school IT facilities will be required to sign a copy of this document and return it to the Network Manager.

The school computer system and all laptops are owned by the school and are available to staff to enhance their professional activities including teaching, research, administration and management. The school reserves the right to examine or delete any files that may be held on the computer system and to monitor any internet sites visited.

This policy has been drawn up to protect all parties – the staff, the students and the school.

- Access should only be made via the authorised account and password, which should not be made available to any other person. Never leave a computer logged on unless you are in attendance.
- All Internet access should be appropriate to staff professional activity.
- Activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Staff must use the RM EasyMail school e-mail address for all official correspondence.
- Any e-mail contact between staff and pupils must only be conducted via RM Easy Mail and the pupils FROG email accounts.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Staff must keep copies of all e-mail correspondence between themselves and parents, ensuring the same professional levels of language and content is applied as in paper based correspondence .
- The school and its facilities will not be used for personal financial gain, gambling, political purposes or advertising.
- Copyright of materials must be respected.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- The introduction of any personal computers/laptops to the school network via a network point or our wireless system is not permitted.
- Staff should not use personal camera phones in school. Digital images of pupils should be stored on the School Network and not on any personal equipment.
- Staff should endeavour to ensure the proper, economical, effective and efficient use of IT resources.

You should be aware that the Network Manager can view your computer screen at any time without your knowledge.

Full Name	Post
Signed	Date

RCI Network Manager /Reviewed by Governing body Mar2014V1

Securing and handling data

This policy should be read as a supplement to the Computer Network AUP.

Staff should not remove or copy sensitive data from the organisation or authorised premises unless the media is encrypted, is transported securely and will be stored in a secure location.

This type of data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc).
Data transfer should be through secure websites e.g. S2S, SecureNet Plus, common transfer files and school census data. If this is not available then the file must be minimally password protected or preferably encrypted before sending via email, the password must be sent by other means and on no account included in the same email. A record of the email should be kept, to identify when and to whom the email was sent.

All school computers will be used in accordance with the Acceptable User Policy signed by all members of staff.

Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. This information must not be stored on a personal (home) computer.

Do not save data files to a PC or laptop other than that provided by the school.

Sensitive data will only be sent electronically through a secure method, e.g. SecureNet Plus. If this is not available then the minimum requirement is to password protect the document before attaching it to email.

Sensitive data includes

Pupil reports	Letters to parents	Exam results
SEN records	Class based assessments	Whole sch data
Medical information	Staff information ie performance management reviews	

If in any doubt as to the sensitivity of data - consider these questions:

Would disclosure / loss place anyone at risk?
Would disclosure / loss cause embarrassment to an individual or the school?
Would disclosure / loss have legal or financial implications?

If the answer to any of these questions is yes, then the data should be treated as sensitive.

I understand that if I do not adhere to these rules outlined in this policy, my network access will be suspended immediately and that other disciplinary consequences may follow including notification to professional bodies where a professional is required to register. If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may be reference for investigation by the Police and could recorded on any future Criminal Record Bureau checks.

In addition, staff should adhere to the 'Clear desk' policy in operation at St Josephs and ensure all sensitive paper records are placed in locked drawers or cupboards.

Name..... Date.....

Data Protection/April 2013/RCL/Governors Review Mar2014

Appendix (iii)

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.