Saint Joseph's
CATHOLIC SCHOOL

E-Safety Policy

Version 2.2 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: Deputy Head / Assistant Head and Network Manager	**When:** Biennially	**How:** Report from Deputy Head / Assistant Head & Network Manager to Governors' Academic Committee

Revision History:			
Version	**Approved and Ratified**	**Review Date**	**Additional Notes**
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:

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

Other SJCS Policies that relate to this Policy:
Child Protection Policy
Safeguarding Policy
Behaviour Policy
Whistleblowing Policy
Staff Code of Conduct
Social Networking Policy (for staff & pupils)

Introduction to the Policy

St Joseph's Catholic school recognises that ICT and the internet are fantastic tools for learning in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography, or face-to-face meetings.

There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our behaviour and anti-bullying procedures which are outlined in our Behaviour Policy.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

The School E-Safety Coordinators are:

- Safeguarding Mr K McGuinness Deputy Head teacher
- Technical Network Manager

The Designated member of the Governing Body responsible for E-Safety is:

- Mr Paul Hooper

Governors

The Academic Governors Committee are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular

information about e-safety incidents and monitoring reports. A member of the Governing body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinators
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors committees

Head teacher and Senior Leaders

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinators.
- The Head teacher and Senior Leaders are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (See Safeguarding & Child Protection Policies).
- The Head teacher and the Designated Safeguarding Lead are responsible for ensuring that the E-Safety Co-ordinators and all other members of staff receive suitable training to enable them to carry out their e-safety roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinators.

E-Safety Co-ordinators

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the E-Safety Governor and or the Pastoral & Ethos Governors Committee to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant committee of Governors
- Reports regularly to the Senior Leadership Team

Network Manager / Technical Staff

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required safety technical requirements and any Local Authority E-Safety Guidance that may apply

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the Head teacher and E-Safety Co-ordinators
- That monitoring software / systems are implemented and updated as agreed with the Head teacher

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and the current school e-safety policy and practices
- They have read, understood, and signed the Staff Acceptable Use Agreement (AUA)
- That they report any suspected misuse or problem to the Head teacher and E-Safety Co-ordinators for investigation / action / sanction
- All digital communications with students / parents / carers should be on a professional level and only carried out using school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and Acceptable Use Agreements
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Leads

Should be trained in e-safety issues and be aware of the potential serious safeguarding / child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues simply that the technology provides additional means for child protection issues to develop.

Pupils

- Are responsible for using the school digital technology systems including Satchel One, Teams and Office 365 in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras
- Will be expected to know and understand policies on the taking / use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take very opportunity to help parents/carers understand these issues through parents' evenings, letters, website, and information about national / local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school
- Their children's personal devices in the school

Communicating School Policy

This policy is available from the school office for parents/carers, staff, and students to access when and as they wish. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities, the website and high-profile events and campaigns e.g. Safer Internet Day.

This policy is also available on our school website. There is also a page dedicated to remote learning.

Training

Staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual on-line e-safety training (through safeguarding refresher training)
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- The E-Safety Co-ordinators will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This E-Safety Policy and its updates will be presented to and discussed by staff on inset days and in meetings
- The E-Safety Co-ordinators will provide advice / guidance / training to individuals as required

Governors:

Governors will be invited to take part in e-safety training / awareness sessions with particular importance for those who are members of any committee involved in technology, e-safety, health and safety and safeguarding / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisations
- Participation in school training / information session for staff or parents

Making use of ICT and the Internet in School

The internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.
Some of the benefits of using ICT and the internet in schools are:

For pupils:

- Online homework platform via Satchel One
- Remote learning through Microsoft Teams
- Unlimited access to worldwide educational resources and institutions such as art galleries, museums, and libraries.
- Contact with schools in other countries resulting in cultural exchanges between students all over the world.

- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.
- Online parents' evenings via SchoolCloud

For parents:

The majority of communication between the school and parents/carers is via e-mail. This form of contact is considered to be more effective, reliable and economic. Text messages and letters will also inform parent/carers of details relating to attendance and behaviour.
Online parents' evenings via SchoolCloud

Learning to Evaluate Internet Content

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

- To be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- To use age-appropriate tools to search for information online
- To acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites, then the URL will be reported to the school E-Safety Co-ordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers, and other external security threats. The security of the school information systems and users will be reviewed regularly by the Network Manager and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.
- Termly reporting to Governors
- Remote access is monitored as per on site

For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

Microsoft Teams & E-mails

The school uses email internally for staff and students, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and students should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Teams is used for setting of assignments, sharing resources, providing feedback on work and communicating with pupils.

School E-mail Accounts and Appropriate Use

St Joseph's Catholic School does not issue student e-mail accounts.

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

- Staff should only use official school-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people for school business.
- Emails and Teams communications sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Published Content and the School Website

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

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights, and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office and named mailboxes (e.g. covid@sjcs.org.uk) only.

Policy and Guidance of Safe Use of Student's Photographs and Work

Colour photographs and students work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material. St Joseph's School believes that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community.

However, we would also like to use photographs and videos of the school and its students externally for promotional purposes (in the public domain) and in order to promote the good educational practice of the school but in accordance with the Data Protection Act 1998 we will only do this with parent/carer consent.

On admission to the school parents/carers will be asked to sign an Acceptable Use Agreement which incorporates digital/video permissions.

By signing this form parents/carers will be consenting to the use of images of their child being used in the following outlets:

- all school publications
- on the school website / school Twitter feed
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects

The form covers consent for the duration of the pupil's time at the school. Once the pupil leaves the school, photographs and videos may be archived within the school.

Student's full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained for external/promotional use.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in school please refer to our **school Safeguarding and Child Protection Policy.**

Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online is detailed in the Social Networking Policy.

Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- They can make students and staff more vulnerable to cyberbullying
- They can be used to access inappropriate internet material
- They can be a distraction in the classroom
- They are valuable items that could be stolen, damaged, or lost

- They can have integrated cameras, which can lead to child protection, bullying and data protection issues. The school therefore adopts a zero tolerance Electronic Device Policy for students during the school day:
- Phones and electronic devices (including headphones) will be confiscated.
- The parents/carer could be contacted and asked to collect the phone/device after the second offence
- The incident will be logged on our behaviour management system.
- Any student who refuses to hand over the complete phone (battery and SIM card) / device when requested will be removed from the lesson. This in turn could lead to a 1 day internal exclusion in the first event and then a fixed term exclusion for repeat offences.
- In circumstances where there is a suspicion that material on a phone is unsuitable the phone will be handed over to the Police for further investigation.
- The school has the right to look at content on devices if there is reasonable suspicion that there is inappropriate content in school. If this is the case, 2 members of staff (one being SLT or a member of the Safeguarding Team) will review the content together in accordance with government guidance.

We do, however, understand that a parent/carer may wish for their child to have a mobile phone for their journey to and from school. In this situation pupils must leave their phone switched off and in their school bag or blazer.

- Emergencies: If a student needs to contact their parents/carers they will be allowed to use a school phone.
- If parents/carers need to contact their child) urgently they should phone the school office and a message will be relayed promptly.

Responsibility:

- St Joseph's Catholic School accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in/confiscated.
- St Joseph's Catholic School will not investigate theft, loss or damage relating to phones/devices.

Staff

- Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time unless in an emergency.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the Behaviour Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying in school does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the Police and service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school. Repeated bullying may result in a fixed-term exclusion.

Managing Emerging Technologies

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

Protecting Personal Data

St Joseph's Catholic School believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect, and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational

needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

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

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example, our local authority, Ofsted, or the Police. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read the school's data protection policy

Unsuitable / Inappropriate Activities

Some internet activity, e.g. accessing child abuse images or disturbing racist material, is illegal and would obviously be banned from school and all other technical systems. Other activities, e.g. cyber–bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the user or the nature of those activities. The school believes that these activities would be inappropriate in our school context:

- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the Catholic ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Using systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Revealing or publicising confidential or proprietary information e.g. financial, personal information, data bases, computer / network access codes and passwords

- Creating or propagating computer viruses or other harmful files
- Unfair usage
- On-line gaming, educational and non-educational
- On-line gambling
- Use of social media without permission
- Use of messaging apps without permission
- Use of videoing broadcasting or YouTube without permission

Responding to Incidents of Misuse

Illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the relevant authorities will be informed.

Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- More than one senior member of staff should be involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- The procedure should be conducted using a designated computer that will not be used by students and if necessary, can be taken off site by the police should the need arise. The same computer should be used for the duration of the process.
- Relevant staff should have appropriate internet access to conduct the procedure, and sites and content visited closely monitored and recorded to provide further protection.
- The URL of any site containing the alleged misuse and the nature of the content causing concern should be recorded. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. This may be printed, signed, and attached to the form (except in cases of child sexual abuse).
- Once fully investigated the group should judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    1. Internal response or discipline procedures
    2. Involvement by Local Authority or national / local organisations (as relevant)
    3. Police involvement and / or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

1. Incidents of 'grooming' behaviour
2. The sending of obscene materials to a child
3. Adult material which potentially breaches the Obscene Publications Act
4. Criminally racist material
5. Other criminal conduct, activity, or material

Isolate the computer in question as best you can. Any changes to its state may hinder a later Police investigation

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the Police and demonstrate that visits to these sites were carried out for child protection purposes.

School Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures (see also E-safety pupil sanctions for inappropriate misuse) and could include:

Pupils:

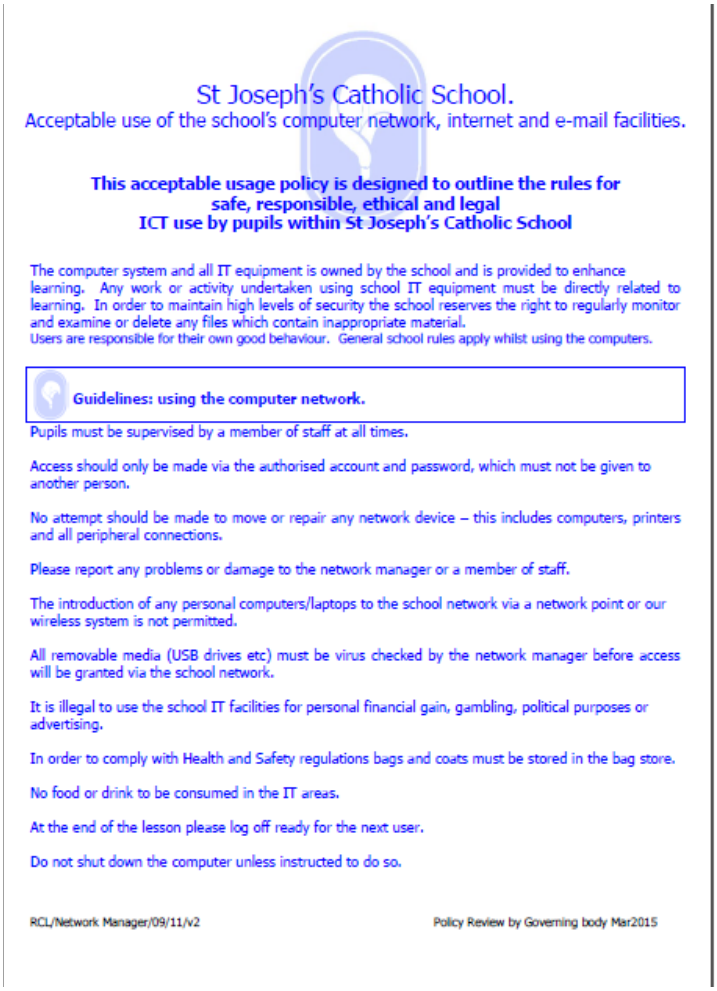
- Referral to class teacher / tutor
- Referral to Head of Department / Director of Learning
- Referral to E-Safety Co-ordinator(s)
- Referral to Line Manager
- Referral to Head teacher
- Referral to the Police
- Referral to technical support staff for action re filtering / security etc.
- Informing parents / carers
- Removal of network / internet access rights
- Risk assessment
- Warning
- Detention
- Fixed Term Exclusion
- Permanent Exclusion/referral to the Fair Access Panel

Staff:

- Referral to Line Manager
- Referral to Head teacher
- Referral to Local Authority / HR
- Referral to technical support staff for action re filtering etc.

- Risk assessment
- Warning
- Referral to agency / counselling
- Suspension
- Disciplinary action
- Referral to the Police
- Dismissal

Pupil Acceptable Use Agreement



St Joseph's Catholic School.
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.

All removable media (USB drives etc) must be virus checked by the network manager before access will be granted via the school network.

It is illegal to use the school IT facilities for personal financial gain, gambling, political purposes or advertising.

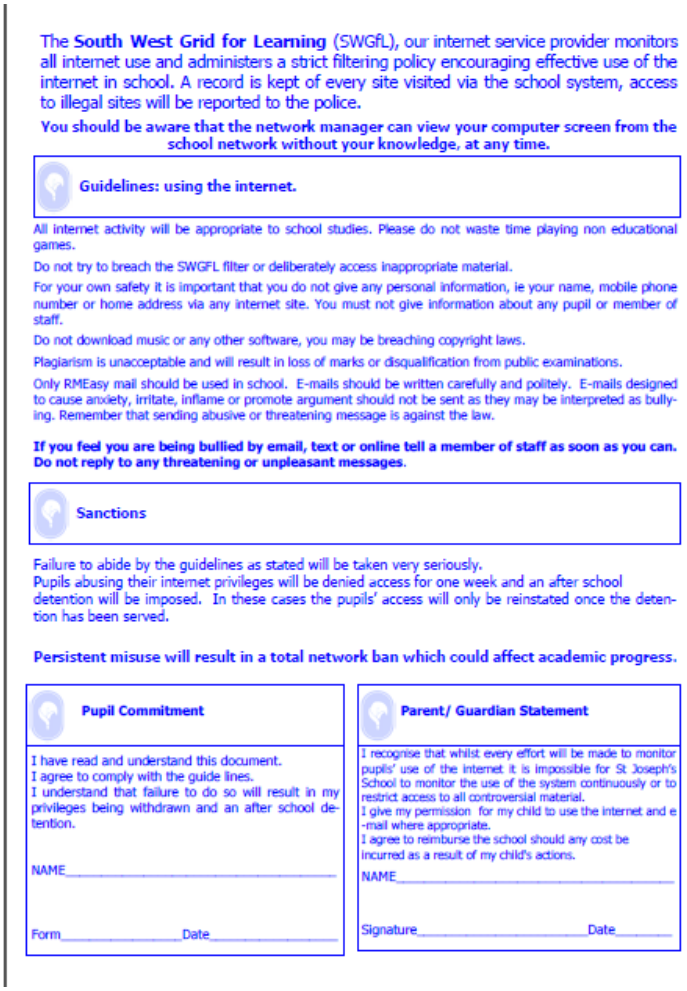
In order to comply with Health and Safety regulations bags and coats must be stored in the bag store.

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.

RCL/Network Manager/09/11/v2 Policy Review by Governing body Mar2015



The **South West Grid for Learning** (SWGfL), 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.

Only RMEasy mail should be used in school. 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.

Sanctions

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.

Persistent misuse will result in a total network ban which could affect academic progress.

Pupil Commitment

I have read and understand this document.
I agree to comply with the guide lines.
I understand that failure to do so will result in my privileges being withdrawn and an after school detention.

NAME_____

Form_____Date_____

Parent/ Guardian 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.

NAME_____

Signature_____Date_____

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

RCl 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 (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.