

St Joseph's Catholic Primary School

Inspiring everyone to **REACH** through Faith, Hope, Love

At St Joseph's, we strive for academic excellence through encouraging resilience, empathy, aspiration and challenge. We have high expectations for ALL so that we can be 'The best we can be.' With Faith, Hope and Love at the heart of our school family, our children feel safe, secure and supported.



Policy for Acceptable Use of ICT & Agreement

Subject Leader:	Hannah Crisp
Link Governor:	
Approved by FGB:	22 nd January 2020
Review due:	July 2021
Other relevant policies:	E-Safety and Safeguarding

Introduction to policy and policy objectives

New technologies have become integral to our lives in today's society, both within their school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe access to the internet and digital technologies at all times.

This policy is designed to keep everyone safe and ensure that all users know their rights and responsibilities when using IT systems, inside school, outside school and when representing the school on any platform.

This policy is divided into sections specifically designed to match each user group with-in the school and as such to clearly define each group's rights and responsibilities.

This policy is to be read in conjunction with the schools GDPR policies available on the school website.

Purpose

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of technology in their everyday work.
- The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

At Saint Joseph's Catholic Primary School, we want to ensure that all members of our community are safe and responsible users of technology.

We will support pupils to:

- Become empowered and responsible digital creators and users
- Use our school resources and technology safely, carefully and responsibly
- Be kind online and help us to create a school community that is respectful and caring, on and offline
- Be safe and be sensible online and always know that you can talk to a trusted adult if you need help

Computer network

- Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, racist, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will result in disciplinary action.

- Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action
- You are responsible for the security of your passwords
- The network must not be used for commercial purposes e.g. buying or selling goods
- Any software / apps installed must be covered by the appropriate licensing agreements
- Copyright of materials available on the network must be respected

Internet / email

- Use of Gloucestershire County Council (GCC) internet and email must be solely for legitimate school purposes
- Use of the internet and email are subject to scrutiny by the school's filtering provider. Any action that might damage the good reputation of the service will be dealt with as a serious act of misconduct
- Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Emails sent from school should contain the same professional levels of language and content as applied to letters or other media
- You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received
- Posting anonymous messages and forwarding chain letters is forbidden
- Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email

Mobile phones

- Professional 'voice' to be used in all phone calls made and text messages sent using work phones
- Personal calls, other than in an emergency, are forbidden on work phones
- Calls and contact to parents / carers should be restricted to the hours of 8.00am to 6.00pm and only using school telephones or mobile phones. An exception may be made in the case of a residential trip in order to inform parents of safety or important information
- Staff must not share their personal contact details

Social Media

Social media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals vulnerable if they fail to observe precautions. This policy is designed to protect staff and pupils from potential harm or from becoming victims of radicalisation, extremism and malicious, upsetting or inadvisable contact. Please refer to Child Protection and Safeguarding Policies available on the school's website.

- All staff should avoid contacting pupils on social networking sites. This is to avoid any possible misinterpretation of motives and the risk of any allegations being made. Pupils must not be added to social media sites for staff.
- Staff social media networks e.g. Facebook, Instagram, Twitter, must not be used in any way which can bring the school into disrepute; this will be dealt with as an act of misconduct
- Staff members **must not** identify themselves as employees of the school in their personal webspace. This is to prevent information on these sites from being linked with the school and

the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services

- Staff members **must not** make contact through any personal ICT or social medium with any pupil, whether from our school or any other school unless the pupil is your own family member OR an existing close family friend.
- Staff **must not** have social media contact with any pupils' family members / carers. This is in line with NASUWT teachers' union and other unions. Teachers should not, for example, accept Facebook requests from parents of a pupil.
- Staff members **must decline** friend requests from pupils.
- On leaving school employment, staff members **must not** contact pupils by means of social media accounts.
- Any information staff members have access to as part of their employment, including personal information about: pupils and their families, colleagues, County Council staff and other parties must not be discussed on their personal webspace or social media sites.
- Photographs, videos or any other types of images of pupils and / or their families or images depicting staff members who can be identified as school staff members must not be published on personal webspace or social media sites.
- School or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access encyclopedias such as Wikipedia in a personal capacity at work. This is because the source of correction will be recorded as the school's IP address.
- School logos or brands must not be used or published on personal webspace / social media sites.
- School does not permit personal use of social media or the internet during core contracted hours, both within school and on visits.
- Caution is advised when inviting work colleagues to be 'friends' on personal networking sites. Social networking blurs the line between work and personal lives.
- Staff **must not** use social media and the internet in any way to attack, insult, abuse or defame: pupils, their family members. Colleagues, other professionals, other organisations, School or County Council - either openly or by suggestion.
- Staff members are strongly advised to set the privacy levels of their personal social media sites as strictly as they can and to opt out of public listings in order to protect their own privacy. Staff members should keep passwords confidential, change them often and be cautious about what is posted online. Staff are advised to take all precautions to avoid identity theft.

Breaches of the policy

- Any breach of this policy may be investigated and may lead to disciplinary action being taken against the staff member/s involved. This is in line with the School Disciplinary Procedure.
- A breach of this policy leading to breaches of confidentiality or defamation or damage to the reputation of the school or any illegal acts or acts that render the school or County Council liable to third parties may result in disciplinary action or dismissal
- Contracted providers of the school must inform the county Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures. Please see GDPR policy and associated Policies.

Children will also be taught, in line with the Computing National Curriculum, about safety online using the following:

Statement for Children

Children will be taught to use the internet a SMART way:

Safe

I ask an adult if I want to use the internet

I keep my information private on the internet

I am careful if I share photos online

I know that if I do not follow the school rules then I will be issued consequences in line with the school's behavior policy, these sanctions will be issued in accordance with the level to which the policy has been broken and are at the digressions on the school's senior leadership and IT Management.

Meeting

I tell an adult if I want to talk to people on the internet

If I meet someone online I will talk to an adult

Accepting

I don't open messages from strangers

I check web links to make sure they are safe

Reliable

I make good choices on the internet

I check the information I see online

Tell

I use kind words on the internet

If someone is not being nice online, then I don't reply, I save the message and show an adult

If I see something online I don't like then I tell an adult.



Acceptable Use Policy & Agreement

I will adhere to the school's Acceptable Use policy.

Name:	
Designation:	Staff / Governor / Visitor / Volunteer (<i>delete as applicable</i>)
Signed:	
Date:	

PRIVACY NOTICE: Please note; we are collecting the personal information you provide above to enable us to maintain an accurate record of your agreement to the school's Acceptable Use policy. This information is protected under our GDPR policies and Privacy Statement. Please see the school website or ask at the school receptions if you would like to know more.