General Welfare Requirement: Safeguarding and Promoting Children's Welfare

Children's behaviour must be managed effectively and in a manner appropriate for their stage of development and particular individual needs.

Safeguarding children

1.12.1 E-Safety

Policy statement for St Joseph's Pre-school
This E- Safety policy reflects the statutory requirements of the Early Years Foundation Stage (EYFS) (latest version) as listed in 'section 3 – The Safeguarding and Welfare Requirements.' This policy and the procedure that it underpins applies to all staff and the Committee, volunteers, students and anyone working on behalf of St Joseph's Pre-school.

At St Joseph's Pre-school we recognise the immense value information and communication technology (ICT) plays in the learning and development of children, we acknowledge that it must be used safely, in that the potential risks involved should not be ignored.

The use of ICT is an essential part of all our lives; it is involved in how we as an organisation gather and store information, as well as how we communicate to each other. It is also an intrinsic part of the experience of our children and young people, and is greatly beneficial to all. However, it can present challenges in terms of how we use it responsibly and, if misused either by an adult or a young person, can be actually or potentially be harmful to them.

Children and young people can be exploited and suffer bullying through their use of modern technology such as the internet, mobile devices, phones and social networking sites. In order to minimize the risks to our children and young people St Joseph's Pre-school will ensure that we have in place appropriate measures such as an acceptable use policy linked to our e-safety policy. We will ensure that staff are aware of how not to compromise their position of trust in or outside of the setting and are aware of the dangers associated with social networking sites.

Our designated person (a member of staff) who co-ordinates child protection issues, **Claire Ajayi**, Deputy Practitioner, supported by staff and the Committee, ensures this policy is upheld by staff and parents alike. St Joseph's Pre-school trusts that all adults will respect and uphold this policy so as to maintain e-safety and prevent any potential risks occurring.

St Joseph's Pre-school aims to:

- Protect children who receive St Joseph's Pre-school's services and who make use of information technology (such as the internet and digital cameras) as part of their involvement with us.
- Provide staff and volunteers with the overarching principles that guide our approach to e-safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

We recognise that:

- The welfare of the children who come into contact with our services is paramount and should govern our approach to the use and management of electronic communications technologies.
- All children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, their parents, carers and other agencies is essential in promoting children to be responsible in their approach to e-safety.

General Data Protection Regulations (2018) (GDPR) and Data Protection Act 2018 (DPA)
Personal data will be recorded, processed, transferred and made available according to the GDPR and DPA, both of which state that personal data must be:

- processed fairly, lawfully and in a transparent manner in relation to individuals;
- obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;
- accurate and, where necessary, kept up to date;
- adequate, relevant and not excessive in relation to the purposes for which it is processed;
- not kept longer than is necessary for those purposes[1];
- protected by appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction or damage; and
- not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

St Joseph's Pre-school's Privacy Notice details what data we collect, how we use it, how we store it and how long we keep it for. A copy of our Privacy Notice can be downloaded from the Pre-school's page on St Joseph's Catholic Primary School's website (www.st-josephs-nympsfield.com).

Staff must make certain that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure data protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.

[1] See policy 5.7 Retention Periods for Records

Procedures

- St Joseph's Pre-school has developed a range of procedures that provide clear and specific directions to staff, parents and volunteers on the appropriate use of ICT. Namely:
    - use of mobile phones, digital photography and recording devices[2];
    - social media[3].
- The use of mobile phones, cameras or electronic communications with a child or family at our setting is only permissible for approved setting business.
- Where it is suspected that a child or young person is at risk from internet abuse or cyber bulling, we will report our concerns to the appropriate agency.
- We use our procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use.

Internet use

- St Joseph's Pre-school has a dedicated laptop which it uses within the setting.
- Internet access is available via St Joseph's Catholic Primary School's network.
- Staff using the computer are made aware that it is password protected and has recognised spyware software installed.
- St Joseph's Pre-school has two Facebook pages[4], one open and one closed[5], and the Social Media policy and procedure covers its use and other social media channels (as applicable). The Facebook page is administrated by the Lead Practitioner and its access is password protected and only known by the Practitioners.

Emails

- St Joseph's Pre-school has designated email addresses for the Chair, Lead Practitioner, Treasurer and Treasury Administrator. All are password protected.
- The Pre-school also has a designated page on St Joseph's Catholic Primary School's website. The Lead Practitioner has permission to change the content of the page. Access to this page is password protected.
- Passwords used by the Chair, Lead Practitioner, Treasurer and Treasury Administrator are not divulged to outside persons. To do so is considered to be a breach of confidentiality and will be treated as such. These passwords are changed when there is a change in Chair.
- The Treasury Administrator has delegated authority to access St Joseph's Pre-school's email address (stjosephspresch@gmail.com) in her capacity of assisting the Chair in his/her role.
- The Treasury Administrator has authority to access the Treasurer's email address (stjosephpstreasurer@gmail.com) in her capacity of assisting the Treasurer in his/her role.

Remote Learning

St Joseph's Pre-school does not use remote learning. However, it encourages its parents/carers to ensure that any electronic equipment, ie. tablet/phone/laptop, that their child has access to, should have suitable parental controls defined. We recommend to our

[2] Policy 1.11 Use of mobile phones, digital photograph and recording devices
[3] Policy 1.12.3 Social Networking
[4] 'St Joseph's Pre-school'
[5] "open" means open to the public, "closed" means group membership, invitation only

parents/carers that they use age appropriate sites and apps and encourage that they visit www.internetmatters.org which provides age related advice in this respect.

We also recommend that parents/carers look at Thinkuknow from NCA-CEOP, which provides support on staying safe online.

Personal emails

- The Pre-school recognises that the Lead Practitioner and Committee will communicate via email outside working hours. The Pre-school advises that personal computers are locked with a security password, and have spyware downloaded as a matter of course.#
- The names of children should be kept to a minimum.
- Correspondence will be written in a polite, respectful and non-abusive manner, with appropriate use of emoticons.
- Any abuse or breeches of confidentiality by any adults/students associated with St Joseph's Pre-school is strictly forbidden, and will not be tolerated.
- All suspected cases must be reported, the Pre-school will record all incidents and act on them immediately.

Storage of documentation

St Joseph's Pre-school recognises that personal computers are used to create working documents for the Pre-school, for examples, registers, invoicing, planning etc.

- All home computers must be password protected.
- All financial documentation with regards to the operation of the setting are stored securely on the Treasurer email GDrive.
- Certain generic documents with regards to the governance of St Joseph's Pre-school are stored securely on the St Joseph's Pre-school email GDrive.
- Work documents placed in locked folders.
- Only acceptable use is permitted.
- Personal details are kept to a minimum.
- All confidentiality is assured, with breaches considered serious misconduct, and dealt with accordingly.

Social media

Please refer to St Joseph's Pre-school's Social Media policy and procedure (Policy 1.12.3). But note that any abuse or breeches of confidentiality by any adults/students associated with the Pre-school is strictly forbidden, and will not be tolerated. All suspected cases must be reported, the Pre-school will record all incidents and act on them immediately.

Use of cameras

Please refer to St Joseph's Pre-school's Use of mobile phones, digital photography and recording devices policy and procedure (Policy 1.11).

Professional photographers

St Joseph's Pre-school uses photographers within the setting in conjunction with St Joseph's Catholic Primary School, this is by arrangement with the staff and Committee.

All photographers have Disclosures and Barring Service (DBS) clearance, are asked for their ID on admission to the Pre-school, and are not left alone with any of the children, at any time.

No photographs of children will be taken without parental consent, and all parents or their named carers are given the option to be present when the photographs are taken.

If no photographs are requested by parents, all proofs are kept by the parents for their safe destruction.

Mobile phones including staff, parents and visitor mobiles
Please refer to St Joseph's Pre-school's Use of mobile phones, digital photography and recording devices policy and procedure (Policy 1.11).

Recording devices (eg. tablets etc)
Please refer to St Joseph's Pre-school's Use of mobile phones, digital photography and recording devices policy and procedure (Policy 1.11).

Reported breeches/complaints/allegations – action taken

- Confidentiality by staff is ensured within their terms and conditions of employment, any reported breech of confidence is considered very serious and could be construed as gross misconduct and which would result in instant dismissal.
- Any complaints or allegations, whether by an adult or a child, will be dealt with according to our Safeguarding children and child protection (including managing allegations of abuse against a member of staff) policy and procedure.

Associated Policies and Procedures

- 1.2 Safeguarding children and child protection
- 1.11 Use of mobile phones, digital photography and recording devices
- 1.2.3 Social Media
- 5.4 Data Protection
- 5.5 Data Subject Access Requests
- 5.6 Data Breach Procedure
- 5.7 Retention Periods for Records
- 5.9 Cloud Computing Services

Further Guidance

- NSPCC online course: *Child Protection: an introduction* [https://learning.nspcc.org.uk/training/introductory-basic-courses]. CPD certified
- DfE Keeping Children Safe in Education (latest version) Paras 134-147 – online safety
- www.internetmatters.org
- Childnet international : Keeping under fives safe online
- Thinkyknow from NCA-CEOP

Version Number	Author	Purpose of change	Date
1.0	K Coupe	New policy	Sept 2014
2.0	K Coupe	To comply with GDPR 2018 & DPA 2018, version control and review	7 Nov 2018
3.0	K Coupe	Policy reviewed. Paragraph on remote learning inserted to comply with requirement in Keeping Children Safe in Education 2020	29/04/2021 Cttee via email (quorate)
4.0	K Coupe	Reviewed in light of updated Keeping Children Safe in Education (Sept 2021). "Further Guidance" section added.	13/10/2021 Chair (A Hitchings)
5.0	K Coupe & A Shipton	Updated re Facebook in line with advice from Early Years Gloucestershire. Clarification between an "open" and "closed" Facebook page	01/02/2022 Cttee Mbr (A Shipton)
6.0	L Farrer & K Coupe	Updated with regards to Treasurer's email address and the use of the GDrive and its adherence to GDPR regulations	27/11/2022 Cttee Mbr (L Finn)
7.0	K Coupe	Updated reference to 1.12.3 Social Media policy/procedure.	09/10/2023 Cttee Mbr (S Webb)