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

1.11.1 Acceptable Use of Technologies

Policy statement for St Joseph's Pre-school
This policy serves to provide a template for the use of technologies within St Joseph's Pre-school that all members of staff, students and volunteers will adhere to for the safe and acceptable use of technologies. This demonstrates compliance with the child protection requirements in the revised Early Years Foundation Stage (EYFS) statutory framework (latest version).

Commitment
Every effort will be made to ensure that this setting's ICT technologies are used in a responsible way, so that there is no risk to the safety or security of the children and adults or to the safety, reputation or sustainability of St Joseph's Pre-school. This applies to the use of technologies on the registered premises of this setting and in any locations visited in connection with the running of the business. It applies to technologies owned by the setting and those owned by others.

[The term 'Technologies' refers to computers/laptops, mini-books, any device with internet access, wearable technology, memory sticks, cameras and equipment that store personal information, databases, electronic records, contact details – this list is not exhaustive].

Purpose
The purpose of having a statement and agreement for the Acceptable Use of Technologies is to provide guidance adhering to the Keeping Children Safe in Education (KCSiE) (latest version) - Annex C guidance to ensure that we highlight risks around Content, Contact and Conduct.

This policy also supports the introduction of "cause and effect" toys, supporting children to understand how basic technology works and can be used within their everyday lives. This progresses to using remote controlled and programmable toys and computers as well as using technology such as cameras.

- Everyone works to ensure that children at St Joseph's Pre-school are cared for and kept as safe as possible, not being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views.
- All adults are responsible users who are pro-active about their own safety and that of the children ensuring no one is subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults.
- All adults are responsible for monitoring personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- The setting's ICT technologies and users are protected from accidental or deliberate misuse which could put St Joseph's Pre-school and its users at risk.

Procedures

- All staff, regular volunteers and students are required to read and sign St Joseph's Pre-school 'Acceptable Use of Technologies' Agreement (see Appendix 1) during their induction into the setting. This signed agreement is retained by the Lead Practitioner or the member of staff's line manager or in the case of a Committee Member, within the Single Central Record and by the signing adult.
- The signed Agreement will be kept, in the case of staff/volunteers, for 6 years after they have left the employment of the setting. With regards to committee members, the Agreement will be kept for 3 years after they have stood down from their role.
- All adults will only use their own user names and passwords which will be carefully chosen so that cannot be easily guessed and no other person will have access or use of this password.
- All adults will ensure that all data (including business documents and files) are regularly backed up.
- All adults will not engage in any on-line activity that may compromise their professional responsibilities or compromise the reputation of the setting or the safety and well-being of the children or staff.
- All adults will ensure that the personal data for any child or family is kept private and confidential in line with current GDPR guidance, except when we are required by law or by the setting's policy to disclose it to an appropriate authority.
- All adults will only transport, hold, disclose or share personal information about themselves or others, in ways agreed by the setting and will not send personal information by email as this is not secure.
- All adults will not send personal data electronically if reasonable security cannot be guaranteed.
- All adults will ensure that there are suitable filtering and security systems in place and that they are not bypassed.
- All adults will ensure that all photos of children cared for by the setting are taken on the setting's camera or tablet. Photos taken on personal cameras, wearable technology or mobile phones must be authorised by the Lead Practitioner. All photos taken must be used and stored appropriately and then deleted from all sources including 'Trash'.
- All adults are required (including visitors and professionals) to not use their mobile phones within the setting and comply with our 'Use of mobile phones, digital photography and other electronic device'[1]. Parents may be asked to refrain from using their phones within the setting. All mobile phones should have their Bluetooth switched off or set to undiscoverable to guard against super Bluetooth jacking.
- All adults will model safe use of the internet and help children to learn to use technologies safely
- Staff are aware of the UKCIS Framework (Education for a connected world) which provides information about the skills and competencies that children need to have with regards to online safety from the age of 4 upwards.
- All adults will take reasonable steps to ensure that the Wi-Fi is disabled on the children's tablets and all use of the internet is supervised, staff will deal with any issues that arise.
- All adults will take immediate action, in line with our setting's policy, if a child reports any concerns or if an issue arises that might compromise the safety of any users, or the security of the setting.

[1] Policy 1.11 Use of Mobile Phones, Digital Photography and Other Electronic Devices

- All adults will communicate online in a professional manner and tone (this includes communication by text message), and will not use aggressive or inappropriate language nor compromise St Joseph Pre-school's reputation.
- All adults will not send or receive personal emails or phone calls when on the premises of St Joseph's Pre-school or use chat or social media sites[2].
- All adults will not access, copy, remove or otherwise alter any other users' files without their permission.
- All adults will ensure permission is obtained to use the original work of others and will credit them if it is used. We will not download or distribute copies of material (including music and videos) which is protected by copyright.
- All adults will only take images of children and staff members where it relates to agreed learning and management activities and will ensure that parent/staff permission is obtained before the images are taken.
- All adults will ensure that, where images are published online or in the media, staff/parent permission is obtained and that these published images (including displays, newsletters, website and prospectus) will not hold any possibility for the identity of any child featured to be identified by name or to find any other personal information about them.
- All adults will ensure that technology equipment is not used to upload, download or access any materials which are illegal and covered by the Obscene Publications Act 1959; or are inappropriate or may cause harm or distress to others.
- All adults will ensure they will only install approved and owned content onto St Joseph's Pre-school's computer/laptops and will not alter laptop or computer settings or open up pop up's or attachments from untrusted sources within the premises of St Joseph's Pre-school.
- At St Joseph's Pre-school events we will ask the audience, in conjunction with previously signed consent forms, if any objections are present for the audience to take photos during the event. If objections are present photos will not be allowed to be taken and Pre-school staff or Committee Members will take photos using the St Joseph's Pre-school's camera and following guidelines previously mentioned. St Joseph's Pre-school holds no responsibility for photos taken by parents.
- Visiting photographers are booked via St Joseph's Catholic Primary School in the autumn term and by the Pre-school in the summer term. All parents have signed parental permission for these photos to be taken and the photos remain protected by the photographer with the agreement of their profession.
- Staff members must ensure that their online personal engagements should be in keeping with their professional status. Images can be checked by visiting 123people.com or via a google search.
- Staff members are required to check their online activity to ensure no unauthorised activity has occurred (e.g. hacking or fraping-Facebook hacking). If unauthorised activity is discovered staff must inform the Lead Practitioner as soon as possible so this breach in their security can be logged.
- Staff are advised (not required) to know their mobiles IMEI numbers so they can dial *#06# if their phone is cloned or stolen.

Tapestry

Tapestry is an online learning diary that will enable St Joseph's Pre-school to give parents/family members instant access to our observations and provide parents/family

[2] Policy 1.12.3 Social Networking

members with the opportunity to comment and share the insights into their child's learning. Both St Joseph's Pre-school and parents/family members can upload photos and videos. Parents/family members will be sent an email whenever an observation is made, meaning parent's get a regular feed of information which can be viewed on a smart-phone or computer. For security parents must complete a Tapestry permission form which details the aim of Tapestry and documents details of who parents have given security access and permission to view their child at St Joseph's Pre-school. If parents/carers would like to alter, add or remove permissions to view their child's learning diary, then they must inform the Lead Practitioner in writing.

Once the child has left St Joseph's Pre-school their learning diary will be removed from our Tapestry site and parents/family will no longer have access to their information.

Key workers have personal log in details and passwords and have read, signed and agreed to a technology code of conduct (see Appendix 1), which stipulates how to keep data secure and confidential. Photos and video will be loaded directly onto the Tapestry site and will not be stored within any laptop or mobile device. In addition Tapestry can be viewed and managed by the Lead Practitioner.

Remote learning

St Joseph's Pre-school does not use remote learning. However, if a child/children are not attending the setting due to, for example, Government guidance (e.g. coronavirus pandemic 2020-21), then the setting will send ideas/activities to parents/carers during their absence. We recommend to our parents/carers that they use age-appropriate sites and apps and advocate that they visit www.internetmatters.org which provides age related advice.

Disposal of IT assets

Disposal of IT assets holding data shall be in compliance with the Information Commissioner's Office guidance[3]. We will ensure that we use an IT asset disposal company which holds the required qualifications when the time comes.

Sanctions

The misuse of the Internet or other technologies may result in disciplinary action and may lead to dismissal, this is at the discretion of the Lead Practitioner and Chair once an investigation has been completed. St Joseph's Pre-school also reserves the right to report any illegal activities to the appropriate authorities.

Legal Framework

- Children Act (1989 s47)
- Protection of Children Act (1999)
- Data Protection Act (2018)
- General Data Protection Regulation (GDPR) (2018)
- The Children Act (2004)
- Safeguarding Vulnerable Groups Act (2006)
- Sexual Offences Act (2003)

[3] See Policy 36: Data collection and information sharing for more information.

- Obscene Publications Act (1959)
- Criminal Justice and Court Services Act (2000)
- Ofsted Whistle Blowing (2014)
- Information sharing (2015)
- Working to Safeguard Children (latest version)
- Childcare Act (2016)
- Ofsted Safeguarding Inspection Guidance (latest version)

Further Guidance

- Early Years Foundation Stage (EYFS) Statutory Framework (latest version)
- DfE's 'Keeping Children Safe in Education' (latest version) - Annex C
- UKCIS Framework

Associated Policies and Procedures

- 1.2 Safeguarding Children and Child Protection
- 1.11 Use of Mobile Phones, Digital Photography and Other Electronic Devices
- 1.12.1 E-Safety
- 1.12.3 Social Networking

Version Number	Author	Purpose of change	Date
1.0	K Coupe	New policy – mentioned in policy 2.1 Employment and Staffing	7 Nov 2018
2.0	T Clapp	Reviewed & amended, added section on Remote Learning	29/04/2021 Cttee via email (quorate)
3.0	K Coupe	Updated reference to Keeping Children Safe in Education (Sept 2021)	13/10/2021 Chair (A Hitchings)
4.0	K Coupe	Reviewed and updated: • minor changes to references to EYFS and KCSiE; • wording relating to children's use of technology; • Inclusion of "Associated Policies and Procedures" section as per EY Safeguarding Audit 2023 S175/157	17/09/2023 Cttee Mbr (S Webb)
5.0	K Coupe	Reviewed and updated as follows: • reference to UKCIS Framework; • inclusion of "wearable technology"; and • amendment to 1.11 Mobile phones, digital photography and other electronic devices.	14/01/2024 Cttee Mbr (G Ind)

Appendix 1

Acceptable Use Agreement: Staff, Volunteers, Students and Committee Members

St Joseph's Pre-school Acceptable Use Agreement is intended to support the online safety of the setting and individual staff, volunteers and committee members through:

- Staff, volunteers and committee members acting responsibly to stay safe while online and being good role models for younger users.
- Effective systems being in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- Staff, volunteers and committee members being aware of how they can protect themselves from potential risk in their use of online technologies.

The term 'professional' is used to describe the role of any member of staff, volunteer, committee member or responsible adult.

For my professional and personal safety I understand that:

- I should ensure that my online activity does not compromise my professional responsibilities, nor bring St Joseph's Pre-school into disrepute.
- My use of technology could be monitored.
- When communicating professionally, I will use the technology provided by the setting (e.g. email). These rules also apply when using the Pre-school's technology (e.g. laptop, email address etc) either at home or away from the setting.
- Personal use of St Joseph's Pre-school's technology is only acceptable with permission.

For the safety of others:

- I will not access, copy, remove or otherwise alter any other user's files, without authorisation.
- I will adhere to current GDPR guidance.
- I will communicate with others in a professional manner.
- I will share other's personal data only with their permission.
- I will use St Joseph's Pre-school's equipment to record any digital and video images, unless I have permission to do otherwise from the Lead Practitioner or Chair.

For the safety of the setting, I understand that:

- I will not try to access anything illegal, harmful or inappropriate.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident.
- I will not share my online personal information (e.g. social networking profiles) with the children in my care.
- I will not deliberately bypass any systems designed to keep St Joseph's Pre-school safe.
- I understand that the Pre-school's Data Protection Policy[4] requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed

[4] Policy 5.4 Data Protection

necessary that I am required by law or by the setting's policy to disclose such information to an appropriate authority.

- I will adhere to current GDPR guidance.
- Personal passwords and those of other users should always be confidential.
- I will not download anything that I do not have the right to use.
- I will only use my personal device(s) if I have permission and use it within the agreed rules.
- I will inform the appropriate person if I find any damage or faults with technology.
- I will not attempt to install programmes of any type on the devices belonging to the setting without permission.

I have read and understand the above and agree to use the settings technology and my own devices when carrying out communications related to the group within these guidelines[5]. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Staff/Volunteer/Student
Committee Member Name: …… [Please print]

Signature: …… Date: ……

[5] Policy 1.11.1 Acceptable Use of Technologies