Safeguarding and Welfare Requirement: Child Protection

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff and cover the use of mobile phones and cameras in the setting.

Online safety at St Clements, use of mobile phones, digital devices and social media including Acceptable Use Policy (AUP)

Policy statement

Digital technologies are powerful tools that open up opportunities for everyone and have become integral to our lives. As a setting we develop a strong culture of safeguarding, one which gives primacy to safeguarding children and encouraging any acts of misconduct to be challenged. We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting. This policy refers to any mobile and/or digital devices (e.g. smart watches, phones, tablets etc) This policy is written with reference to the BCP Council Early years online guidance last updated September 2019. (Appendix 1) All staff sign an Acceptable Use Policy (AUP) when they commence at the setting, Online Safety training forms part of the initial induction and thereafter staff receive regular updates on Online safety. The setting reviews its practice regularly, informed by best practice and emerging threats through the use of improvement tools.

EYFS themes and principles underpinning policy and practice. (Learning and Development)

A Unique Child (UC)	Positive Relationships (PR)	Enabling Environments (EE)
Every child is a unique child who is constantly learning & can be resilient, capable, confidant & self-assured	Children learn to be strong and independent through positive relationships.	Children learn & develop well in enabling environments, in which their experiences respond to their individual needs & there is a strong partnership between practitioners & parents

Procedure

Our designated person responsible for co-ordinating action to protect children is Elaine King. As DSL she has the overall responsibility, monitors incident logs, and responds to any safeguarding concerns. Our named Online Champions are Paige Burry (Nursery), Mike Hills (Nursery), Sabina Krzynowy (Iford) and Sara Dawson (Administrator). Our Online Champions will be responsible for ensuring that all staff are kept up to date with online safety information and work in a collaboration with the DSL. They will contribute to the development and review of these policies and procedures and will ensure these are shared with all staff. They are aware of online safety issues and potential for serious safeguarding issues and can manage them effectively. The outcomes of these incidents should be used to inform and improve online safety policy and practice. An audit of online safety training of all staff will be carried out regularly.

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- We monitor the use of these devices and how they are used through supervision.

- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.
- All devices and networks used professionally can be accessed through secure passwords assigned to individual appropriate users.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
  - only go on line with a grown up
  - be kind on line
  - keep information about me safely
  - only press buttons on the internet to things I understand
  - tell a grown up if something makes me unhappy on the internet
- Qualified practitioners will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships and asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.
- All devices for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- Staff and volunteers will act as good role models in their use of online technologies.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk**.**
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.
- We will seek to provide parents/carers with increased awareness of online safety through our website and through informal discussion. Where possible we will signpost to relevant information/websites for parents/carers.

Email

- Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Staff send personal information by encrypted email and share information securely at all times.

Cameras and digital devices

- Our staff & volunteers must not bring their personal cameras or digital devices into the setting. All devices used in the setting for the purpose of taking photographs and video recordings, must be kept secure and usage monitored, and images deleted regularly.
- Photographs & recordings of children are only taken for valid reasons i.e. to record their learning and development, or for displays within the setting, with written permission received by parents (see the Registration form). Such use is monitored by the manager using equipment belonging to the setting.
- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have a right to photograph anyone else's child or to upload photos of anyone else's children.
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name or through being photographed in a sweatshirt with the name of their setting on it.
- Digital images are stored in accordance with the Data Protection Act 2018 and GDPR 2018.

Social media

- We request that anyone accessing the setting respects our confidentiality policy, including parents.
- Any information that directly or indirectly relates to the setting, including photographs, are **not** shared on social networking applications. Failure to follow this may be in breach of the settings confidentiality policy and would be dealt with accordingly.
- Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- Staff should not accept service users, children and parents as friends due to it being a breach of expected professional conduct. Remember staff members/volunteers are an ambassador for our setting and so their personal and professional lives should be kept separate.
- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity.
- If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.
- In the event that staff names the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.
- Staff observe confidentiality and refrain from discussing any issues relating to work. See Confidentiality Policy and Disciplinary Procedure.
- Staff should not share information they would not want children, parents or colleagues to view.

- Staff should report any concerns or breaches to the designated person in their setting.
- We have both a website and a Facebook page. These are used for professional purposes to inform our parents/carers of key information. We will not publish photos of children who attend or have attended our settings on our website in order to safeguard them. We do not usually use photos of children on our Facebook page, if any photos are used the children will be unidentifiable. We never share names full or otherwise of children on any public facing media.
- Our Facebook page is regularly monitored for concerns/complaints and comments responded to. It is used to connect with our audience and reach potential customers.
- Access to the management of the Facebook Page is restricted to the directors. They ensure there is a secure login/password and manage what is posted. They will also respond to any private messages.
- Our website is regularly updated.

Mobile phones – children

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in a locker until the parent collects them at the end of the session.

Mobile phones and connected watches/wearable devices – staff and visitors

- Personal mobile phones are not used by our staff on the premises during working hours. They will be stored securely, away from children and locked away from any access during sessions.
- If a member of staff/volunteer has a wearable device such as a watch that requires Bluetooth, we require them to disconnect the Bluetooth when they are putting away their phones in the lockable cupboard to ensure that they are safe to wear. Or the watch can be put into do not disturb mode.
- In line with safer working practices, staff must not use their personal mobile phone to contact parents.
- In line with safer working practices, staff must not give their personal contact details to parents.
- In an emergency, personal mobile phones may be used in a “Supervised phone zone” where there are no children present, with permission and /or supervision from the manager.
- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- Staff must not have inappropriate or illegal content on their mobile phone. You have a duty to report any camera and image, mobile phone or Online safety incident which may impact on you, your professionalism or your organisation.
- If our members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- Parents and visitors are requested not to use their mobile phones whilst on the premises. We make an exception if a visitor’s company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a supervised phone zone where they can use their mobile phone, where no children are present.
- There is clear signage regarding the mobile-free areas of our settings.

- Think about responsible use of location apps on mobile phones, these may display the location of the setting and are sometimes automatically activated.
- The settings mobile phone has the appropriate security settings including passwords and only authorised users have access to it.
- These rules also apply to the use of work-issued mobiles, or when visiting or supporting staff in other settings.

Electronic learning journals for recording children's progress

- Our setting uses digital images and video as a tool to record and inform parents/carers of the progress of their children. It may be used to support multi agency working with professionals. The devices we use for recording images of children are provided by the setting for staff/volunteers to use professionally.
- We use a reputable provider, Foundation Stage Forum LTD for Tapestry which can guarantee the security of the data put on the system.
- A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Only the managers and those we authorise can access Tapestry, be that staff and parents.
- Staff have Pin only access meaning that they can not log in without a manager logging in first.
- Privacy notices are shared with parents/carers so that parents are clear on how/why images are stored/recorded and why they are needed. Appendix 2
- We must ensure we are compliant with data protection law and adhere to the principles of GDPR that data we hold is for a legitimate purpose, processed lawfully, accurate, up to date and kept for no longer than necessary.
- Parents have the right to refuse and withdraw consent for their use at any time.
- Parents are also advised how to access/protect their children's data by using strong passwords and not sharing them.
- Staff always adhere to the guidance provided with the system and are made aware which of their personal data are added.
- Staff member access is deleted when they leave the setting.
- The Electronic learning journal file for the child is deleted when they leave the setting.

Use and/or distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.
- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

Responding to issues

Our setting can recognise online safety issues when they arise and there is clear guidance and established procedure to respond to them. Procedures are in place to identify, manage and escalate incidents as they arise. We will respond to and act upon any reports of online safety breaches. Any concerns/issues be it from staff or parents or any members of the community should be reported to the setting in the first instance. They then may be escalated through the appropriate channels if necessary. Where illegal misuse has been identified it is immediately reported to the DSL and escalated through the setting's safeguarding procedures to the appropriate supporting agency. (Police, Multi Agency Safeguarding Hub). Where we may suspect that misuse may have taken place, but it is not illegal, we will investigate, preserve evidence, and protect those carrying out the investigation. Incidents of misuse by staff/volunteers will be dealt with through agreed disciplinary procedures.

Further documentation reference
Information sharing policy
Whistle blowing policy
Confidentiality policy
Contracts of employment

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/
- Pan Dorset Safeguarding Children Partnership multi-agency procedures
- EYFS Statutory framework
- BCP Provider Agreement

Useful contacts, resources, and websites

- UK Safer Internet – Advice Centre
- Making a Report to CEOP
- Think U Know education programme
- NSPCC – Online Safety
- Bournemouth and Poole LSCB – Safer Internet Use
- Dorset Safe Schools and Communities Team
- Childnet International
- Vodafone child online safety
- Childline – Online Safety
- Common Sense Media
- Safety and Security Online - SWGfL
- Digital Parenting – Protect your family

- Parent Zone – experts in digital family life

CCTV and data protection guidelines

- Guidance on the use of domestic CCTV – GOV.UK
- Data Protection – GOV.UK
- Information Commissioner's Office

Safe search engine support

- Parental Controls - Childnet
- Appropriate Filtering and Monitoring – UK Safer Internet

This policy was adopted by	St Clements
On	Spring Term 2021
Date to be reviewed	Spring Term 2022
Signed on behalf of the provider	
Name of signatory	Sara Dawson
Role of signatory (e.g. director or owner)	Online champion

Full policy review undertaken by whole team feedback and parental feedback. Spring 2018

Policy reviewed with 360 Early Years Audit Tool used by Sara Dawson November 2020

www.360earlyyears.swgfl.org.uk

Appendix 1

https://www.bournemouth.gov.uk/childreneducation/working-in-childcare/early-years-safeguarding/safeguarding-documents/amended-bcp-online-safety-guidance-september-2019.pdf