



Safeguarding children, young people and vulnerable adults' procedures

E–Safety (including all electronic devices with imaging and sharing capabilities)

Policy Statement

Cricklade Pre-School Playgroup has a commitment to keeping Children safe and the E-Safety Policy operates under the umbrella of the Safeguarding Policy.

We take steps to ensure that there are effective procedures in place to protect children from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

An E-safety audit is included in these procedures to assist with compliance to the EYFS.

Procedures

□ Our designated persons responsible for co-ordinating action taken to protect children are:

Ann Uzzell and Di Barton

Children at Cricklade Pre-School Playgroup do not have Internet access on their computers.

However, staff do discuss with Children the need to be safe when using computers and tablets at home and only accessing games which their parents have agreed.

- 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

Staff role model safe behaviour and privacy awareness and talk to children about safe use.

Staff also discuss with parents the need to ensure their Child's safety on-line by using appropriate parental locks.

Website/E-mail

The point of contact on our website will be the Pre-School address, Pre-School e-mail and telephone number.

Staff or Children's home information will not be published. Website photographs that include children will be selected carefully and only used with parents specific permission. Pupil's names will not be used anywhere on the website.

Staff using e-mail will use a Pre-School e-mail address. This address must not be used for personal e-mail.

On line chat rooms will not be used at the preschool.

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- Screen based assistive technologies may be used to support staff or children in the setting on a case-by-case basis
- The setting manager will regularly spot check devices to ensure they are being used safely and securely.
- Families are informed of how the setting is supporting children's use of technology.
- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Tablets remain on the premises and are stored securely at all times when not in use. Staff follow the additional guidance provided with the system.
- The designated persons are 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.
- If a second-hand computer is purchased or donated to the setting, this will be checked to ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- 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.
- 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 on line is an offence in its own right
- and concerns about a colleague's or others' behaviour are reported (as above).

Personal mobile phones and other internet-enabled devices – staff and visitors

- Personal mobile phones are not used by staff in the room at Cricklade Preschool Playgroup during working hours. Personal mobiles and other internet enabled devices may be used in a safe place e.g., staff room or office. The setting manager completes a risk assessment for where they can be used safely. This includes smart watches and meta glasses.
- Personal mobile phones are stored in their personal drawers in the office.
- In an emergency, personal mobile phones may be used in the privacy of the office with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Staff do not take their mobile phones or other internet enabled devices on outings away from the preschool however they will take the settings mobile phone with them for safety reasons.

- Parents/carers and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day phones still should be stored away from any areas that children access and setting phone number given to visitors so that they are still contactable. Visitors are advised of a private space where they can use their mobile.
- Medical evidence is required for an exemption such as diabetes where the phone is used to alert the staff member of reduction in sugar levels. Any electronic devices which are used to manage medical needs must be agreed with the manager. A risk assessment for the storage and management of devices is completed by the manager.
- No photos or video should be taken on personal mobile phones, smart watches or any other electronic device with imaging and sharing capabilities by either parents or staff.

Cameras and videos

- Members of staff at Cricklade Preschool Playgroup do not bring their own cameras or video recorders to the setting. They do not use their own personal phones to take any images or videos.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting. Children are given the opportunity to consent to their photograph being taken, even if parent/carer permissions are in place.
- Camera and video use is monitored by the setting manager or designated safeguarding lead.
- Where parents/carers request permission to photograph or record their own children at special events, general permission is first gained from all parents/carers for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- All photographs at Cricklade Preschool Playgroup are printed on setting equipment and **should not** be outsourced for printing to an external company.
- Photographs/recordings of children are only made if relevant permissions are in place by parents or guardians. We will advise parents of why we are capturing the image, the security measures that are in place to safely store the image and devices used, how long it will be kept for and how.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.
- Photographs and Image scraping:
Cricklade Preschool Playgroup recognises that although some apps and websites provide the option of covering children's faces with emojis and stickers, with the development of AI tools, these can be reconstructed with highly accurate facial likeness. Any photographs used for publicity, will have parent consent and safeguarding risks minimised by ensuring that children are not able to be identified.
Using stickers and emojis, to protect children's privacy, can be removed or bypassed using editing tools and technology such as image scraping. This means a child's face can still be identifiable or recoverable.

Policy no:1g

- Photographs taken of children at Pre-school will not be used on the Pre-School web pages.
- Photographs stored on the Pre-school computer will be retained for a maximum of two years.
- Pre-School will not give digital copies of photographs to parents or third parties.
- A professional photographer may be invited to Pre-School occasionally to take individual photos of the children; these photos are for the parents if they wish to buy them. Copies will not be retained by the Pre-School.

CCTV

Cricklade Preschool Playgroup has chosen not to use CCTV within its setting. The nursery believes that effective safeguarding is best achieved through robust recruitment practices, appropriate staff-to-child ratios, active supervision, regular training, strong leadership oversight, open communication with families, and an embedded safeguarding culture.

The nursery recognises that CCTV can provide additional security benefits; however, we have concluded that the potential impact on the privacy of children, staff and visitors outweighs the benefits in this particular environment. The nursery is committed to creating a warm, safe and nurturing atmosphere where children can learn and develop without routine surveillance.

To ensure safeguarding remains effective, the nursery maintains comprehensive safeguarding policies and procedures, regular risk assessments, clear reporting mechanisms for concerns, and ongoing monitoring of practice by managers and leaders. These measures provide assurance that children's welfare remains the highest priority while respecting the dignity, privacy and rights of all members of the nursery community.

The decision not to use CCTV is reviewed periodically to ensure it continues to reflect the nursery's safeguarding needs, legal responsibilities, and the best interests of children, families and staff.

Social media

Cricklade Pre-School Playgroup recognizes that many employees, parents and carers use the internet for personal purposes and that they may participate in social networking on websites such as Facebook, Myspace, Twitter etc. In addition employees, parents and carers may set up personal weblogs or "blogs" on the internet.

Whilst everyone is free to use the internet for social networking, they must ensure that they do not breach the law or disclose Cricklade Pre-School Playgroup's confidential information, breach copyright, defame the Pre-School, its children or parents or other employees; or disclose personal data or information about any individual that could breach the Data Protection Act 1998 and to keep completely confidential any information regarding the children, their families or staff members which is learned through pre-school.

This policy relates to material posted on public areas and those restricted to certain individuals.

Procedures

As an Employee and for the protection of your professional reputation, it is expected staff comply with the following procedures:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure Cricklade Preschool Playgroup is not negatively affected by their actions and do not name the setting
- be aware that comments and photographs may be accessible to anyone and staff should use their judgment before posting. Imagine that all work contacts are all able to visit the site. It is not like

posting something on your web site or blog and then realizing that a story or photo should be taken down. On a social networking site, basically once you post something it may be available, even after it is removed from the site.

- do not discuss children, parents or co-workers or publicly criticize the setting policies, activities or personnel.
- be aware that images, such as those on Snapshot may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- do not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to access
- do not accept service users/children/parents as friends, as it is a breach of professional conduct. Pre-school will make an exception to this rule if an employee has an existing relationship with a child's parent(s) before that child starts at Pre-School. This rule no longer applies once a child has left Pre-School.
- report any concerns or breaches to the designated safeguarding lead in their setting
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the educator and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed
- Do not write or respond to anything deemed to be defamatory, obscene, proprietary, or rebellious. Exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions and derogatory remarks or characterisations.
- Consider whether a particular posting puts your effectiveness as a childcare professional at risk.
- Refrain from identifying yourself as working for the pre-school.
- Take care not to allow interaction on these websites to damage working relationships between members of staff and parents of the pre-school.
- Do not conduct yourself in a way that is detrimental to the Pre-School.
- Remember that people classified as 'friends' have the ability to download and share your information with others.

Parents, Carers and Employees should also comply with the following procedures:

- Do not use the pre-schools website, internet systems, e-mail addresses or intranet for your own weblog.
- Do not link personal websites to the pre-school's website or disclose the name of the preschool on it or allow it to be identified by any details.
- Do not disclose any information that is confidential to the pre-school. The Pre-School's confidentiality policy provides guidance about what constitutes confidential information.
- If anyone chooses to write about their experience at Pre-School, even without identifying it, it may be possible to work out the pre-school's identity. Everyone should always be conscious of their duty to act in good faith and in the best interest of the pre-school under English Law.
- The pre-school will not tolerate criticisms in any web posting; even where they are true and not defamatory.

Policy no:1g

These amount to a breach of the child's registration / employee's contract and could lead to the withdrawal of the child from pre-school or to action under the Pre-School's employment and staffing policy.

- The Pre-School's complaints policy aims to provide guidance to all those who work with or within the Pre-School, or someone with issues they wish to raise with pre-school.
- Do not discuss children's progress or activities on networking sites.

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague at Cricklade Preschool Playgroup is behaving inappropriately, staff advise the designated safeguarding lead who follows the procedure for allegations against staff, volunteers or agency staff.

Cyber bullying

Cricklade Pre-School Playgroup is committed to ensuring that all of its staff, parents and carers are treated with dignity and respect. Bullying and harassment of any kind will not be tolerated.

Cyber bullying methods could include text messages, mobile phone calls, instant messenger services, circulating photos or video clips or by posting comments on websites blogs or chat rooms. Employees, parents or carers who cyber-bully could face criminal prosecution.

Action

If necessary, action will be taken against any employee, parent or carer who is found to have breached this policy.

Security Advice

Employees, parents and carers should be aware that social networking websites are a public forum. Employees, parents or carers should not assume that their entries on any website will remain private. Visit your profiles security and privacy settings. At a minimum, childcare professionals should have all privacy settings set to 'Only friends'.

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-cando/get-expert-training/keeping-children-safe-online-course/
- Safeguarding Children (Early Years Alliance)
- <https://help-for-early-years-providers.education.gov.uk/health-and-wellbeing/screen-use>
- <https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings>
- [Help for early years providers: Internet safety](https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations)
<https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations>
- https://www.internetmatters.org/advice/0-5/#checklist_for_preschool
[Online Safety in the Early Years | LGFL](https://www.internetmatters.org/advice/0-5/#checklist_for_preschool)

Agreed by the committee of Cricklade Pre-School Playgroup



Technology used in our setting (Add the types and numbers of devices)	ICT Equipment Computers (office) Computers (children) iPad (staff/children) Cameras/videos Electronic learning journals Nursery Management Software Other.	Quantity Office computer x 1 Lap Top x 1 Camera x 1 Tablets x 6 Tapestry and Superfox	Wi-fi enabled Yes or No? Yes	Security settings i.e. passwords, firewalls, screen locks etc.. Password protected Microsoft account protection and Firewall and Network Protection	Who has access? Office computer - Manager and Admin Lap top – with permission Tablets/camera – all staff
Policies and Procedures – name of policy, or policy in which it is incorporated.	Subject - Acceptable use: <u>Yes/No</u> - Staff use of social media <u>Yes/No</u> - GDPR/Data Protection <u>Yes/No</u> - Personal mobile phones / wearable technology		Policy/ Procedure E-Safety Policy Social Networking Policy Privacy Policy Photography/ Mobile Phone and Camera Policy	Further action required Continue to review and update when required	
Approved Apps/websites/online tools.	<i>List the apps/websites/online tools that you use in your setting with the children</i> N/A				
How are children supervised when using devices?	Please give details here... N/A				

How is the physical safety of users managed, i.e. posture, time spent on devices	Please give details, including, posture, time spent on devices etc. N/A
How are devices stored securely when not in use?	Please give details.... All devices are logged out and stored in a locked cabinet PC/Lap top are logged off
How do staff model safe practice when using technology with children?	Please give details... By discussing the safe principles with the children as per the E-Safety policy
How is internet safety and use of technology incorporated into the early Years curriculum?	Please give details... Policies and discussions
How is the home learning environment supported?	Add details of information shared with parents to support safe internet use at home. All policies are shared with parents and any relevant updates
Resources to support Internet safety in early years provision.	• http://internetmatters.org/ • <u>Online safety guide 0-5 year olds - Internet Matters</u>