

Safeguarding children, young people and vulnerable adults procedures

E-safety (including all electronic devices with internet capacity and with imaging and sharing capabilities)

This policy is to safeguard both staff and children within the setting. This policy should be read in conjunction with the Child protection and Safeguarding Policy and the Acceptable Use policy.

There will always be risks when using any form of communication that lies within the public domain. It is essential that clear rules, procedures, and guidelines are in place to minimise risk.

**Online Safety**

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as ‘e-safety’, ‘online’, ‘communication technologies’ and ‘digital technologies’ refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks.The issues are:

*Content* – being exposed to illegal, inappropriate or harmful material

*Contact* – being subjected to harmful online interaction with other users

*Conduct* – personal online behaviour that increases the likelihood of, or causes, harm

**I.C.T Equipment**

Frimley Green Pre-School does not currently have tablets/ipads.

* The setting supervisor ensures that all computers have up-to-date virus protection installed.
* Computer equipment is password protected.
* Tablets/Cameras are only used for the purposes of observation, assessment, and planning and to take photographs for individual children’s learning journeys.
* Tablets/Cameras remain on the premises and are stored securely at all times when not in use (supervisor’s drawer).
* Staff follow the additional guidance provided with the system.
* The Supervisor, Deputy and DSL will endeavour to ensure E-safety will be managed and implemented effectively. They may need to obtain the necessary advice from ICT experts regarding system security and virus protection.
* Safeguarding is everybody’s responsibility and therefore an agreed, shared approach must be promoted by all.

**Internet access**

The pre-school has access to the internet through the community centre WiFi. Access to the internet is via a password provided by the community centre.

* Children never have unsupervised access to the computers or the internet.
* The setting supervisor assesses the risk in relation to e-safety.
* Only reputable sites with a focus on early learning are used (e.g. CBeebies).
* Children are taught the following stay safe principles in an age-appropriate way:
* only go online with a grown up
* be kind online **and** 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 support children’s resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
* The children do not have unsupervised access to the computer. 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](http://www.iwf.org.uk/).
* Children will not bring their own internet devices, games consoles, etc into the setting.

The setting supervisor ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

**Personal mobile phones also including all electronic devices with imaging and sharing capabilities – staff and visitors** (includes all internet enabled devices)

* Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e,g, kitchen.
* Personal mobile phones are stored in a box in the kitchen.
* Smart watches may be worn but must be disabled from the internet when inside the setting.
* In an emergency, personal mobile phones may be used in the privacy of the office/kitchen with permission.
* The setting supervisor has access to a mobile phone for receiving authorisation codes to access the Early Years Funding Portal (this phone does not have a camera or recording device).
* Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
* Members of staff do not use personal equipment to take photographs of children.
* Parents and visitors do not use their mobile phones on the premises. Visitors are advised of a private space i.e. the kitchen, corridor where they can use their mobile.
* Parents should only contact staff members on the pre-school telephone or via the pre-school email address only.
* For safeguarding and safety reasons, staff will not release the children to parents/carers using their mobile phones when collecting their children at the end of the session.

**Cameras and videos (including all electronic devices with imaging and sharing capabilities)**

* 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.
* Camera and video use is monitored by the setting supervisor.
* Where parents request permission to photograph or record their own children at special events, parents are told they do not have a right to photograph or upload photos of anyone else’s children.
* Photographs/recordings of children are only made if relevant permissions are in place.
* If photographs are used for publicity, parental consent is gained, and safeguarding risks minimised.
* Staff downloading photos from the camera for their key children’s files will inform the supervising member of staff before doing so. The camera SIM card must be replaced in the camera after the download.
* Camera and video equipment must not be taken into the toilets.

**Cyber Bullying**

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 [www.nspcc.org.uk](http://www.nspcc.org.uk) or ChildLine Tel: 0800 1111 [www.childline.org.uk](http://www.childline.org.uk)

**Use of social media**

Staff are expected to:

* understand how to manage their security settings to ensure that their information is only available to people they choose to share information with.
* ensure the organisation is not negatively affected by their actions and do not name the setting.
* are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting.
* are 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
* 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
* not accept service users/children/parents as friends, as it is a breach of professional conduct
* 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 supervisor and a risk assessment and agreement in relation to boundaries are agreed.
* Pre-School Facebook will be administered by the Supervisor or administrator and will follow the same protocol as the website.

**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 is behaving inappropriately, staff advise the designated safeguarding lead who follows procedure Allegations against staff, volunteers, or agency staff.

 **Website**

* The pre-school has a website address which is [www.fgps.co.uk](http://www.fgps.co.uk) . The supervisor and administrator can currently make changes to the site. Any photographs displayed will be in line with pre-school policy.
* The administrator must ensure that all files on the computer involving pre-school data are password protected and that confidentiality is maintained.

**Emails**

The general pre-school email address is fgpsenquiry@gmail.com. However, the Designated Safeguarding Lead will use dsl.fgps@gmail.com for sensitive emails regarding child protection matters. The administrator may use fgpsoffice@gmail.com for sending invoices and financial matters.

From time-to-time staff members may communicate with each other by personal email. The supervisor and DSL may circulate updates from Surrey Safeguarding Children’s Board, Early Years Information, Minutes of meetings etc. All staff members must ensure that information sent to them about Frimley Green Pre-School remains confidential.

Sensitive information between other agencies e.g. social workers, speech and language therapists, will be sent using the secure egress platform.

**Parent involvement**

Parents are encouraged to keep their children safe online. Information and advice can be found on [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk). Important information and updates will be distributed to parents by newsletter Any updates will be communicated to staff via meetings or newsletters.

****This is the CEOP symbol, and it is on some websites accessed by children. Children should be encouraged to click on this icon if they begin to feel uncomfortable online and it will alert the police to the problem.

**Reporting criminal online content**

You can report criminal online content to the Internet Watch Foundation www.iwf.org.uk or to CEOP www.ceop.police.uk/report-abuse. Reports are confidential and can be submitted anonymously.

If we become concerned about a child being involved in online abuse, then the Child Protection Policy will be followed. The Contact Centre Children’s Team will be contacted for advice telephone 0300 470 9100.

If we become concerned about a staff member being involved in online abuse, then the Child Protection Policy will be followed, and the Local Area Designated Officer (LADO) will be contacted for advice on telephone 0300 123 1650.

All concerns should be written up on report forms in the Child Protection file and stored in the locked confidential box in the office.

PLEASE NOTE where indecent images of children or other unsuitable material are found it is important that individuals do not investigate the matter or evaluate the material, as this may lead to evidence being contaminated which can lead to criminal prosecution. Always contact the relevant advice teams.

**The legal framework surrounding e-safety**

The Computer Misuse Act 1990 (sections 1-3)

Copyright, Design and Patents Act 1988

Data Protection Act 1998

Malicious Communications Act 1998 (section 1)

Obscene Publications Act 1959 and 1964

Public Order Act 1986 (sections 17-29)

Protection of Children Act 1978 (section 1)

Protection from Harassment Act 1997

The Equality Act 2010

Regulation of Investigatory Powers Act 2000

Sexual Offences Act 2003

**Useful websites:**

www.thinkuknow.co.uk

www.childnet.com

www.besafeonline.com

Www.wisekids.org.uk

www.education.gov.uk/ukccis

www.saferinternet.org

www.safenetwork.org.uk

www.ceop.police.uk

www.ico.org.uk

www.childline.org.uk

[www.nspcc.org.uk](http://www.nspcc.org.uk)

This policy was amended on 1st February 2024

Reviewed by……………………………………..Date…………………………………..

Reviewed by……………………………………..Date…………………………………..

Reviewed by……………………………………..Date……………………………………….