Spilsby Playgroup

Online Safety and Acceptable Use Policy

Including devices with imagery and sharing capabilities

2026

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

Aim

For Spilsby Playgroup to ensure:

- All children remain safe
- Safe and appropriate use of technological resources including, personal devices, wearable technology, mobile phones and cameras
- Acceptable and appropriate use of technology within the setting;
- Expectations are clear regarding professional boundaries/behaviour of staff, including communication via social media
- Policies and procedures are easily accessible to staff and parents/carers
- To support parents in having the knowledge to help protect their child when online.

An E-safety audit is included in these procedures (see Appendix 1) to assist with compliance to the revised EYFS 2025.

Online Safety

It is important that children and young people attending Spilsby Playgroup receive consistent messages about the safe use of technology and can 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

- The manager at Spilsby Playgroup ensures that all computers have up-to-date virus protection installed.
- Tablets are only used by educators at Spilsby Playgroup 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 always stored securely when not in use.
- Staff follow the additional guidance provided with the system

Internet access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- 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 at Spilsby Playgroup 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.
- All computers for use by children are sited in an area clearly visible to staff.
- 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.

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

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Make use of home visits to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-

years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not used by staff Spilsby Playgroup during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e.g., staff room. The setting manager completes a risk assessment for where they can be used safely.
- Personal mobile phones are switched off and stored in lockers or a locked office drawer.
- 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 on outings.
- Members of staff do not use personal equipment to take photographs of children.
- 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.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.
- 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.
- 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.
- 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, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

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 or ChildLine Tel: 0800 1111 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 Spilsby Playgroup 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 manager and a risk assessment and agreement in relation to boundaries are agreed

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 Spilsby Playgroup is behaving inappropriately, staff advise the designated safeguarding lead who follows procedure 06.2 Allegations against staff, volunteers or agency staff.

All staff:

- Understand their safeguarding responsibility and are clear about how the 'Acceptable Use Policy' fits into their role on a day-to-day basis. This includes the taking of photographs as a part of their child's online profile via Tapestry.

- Have completed safeguarding training as a part of their staff induction and completed refresher training annually
- Are aware, communication with parents/carers and colleagues should be professional and take place via official setting communication channels e.g. work provided emails/numbers to protect both staff and children
- Communication should be transparent and open to scrutiny
- Understand that it is recommended that staff do not accept friend requests or communications from children (past or present) family members (past or present). If there is a pre-existing relationship, this should be discussed with the DSL and/or the manager, who will need to consider how this is managed, provide staff with clear guidance and boundaries and record action taken.
- Are aware that if they or another member of staff are targeted online, for example online bullying or harassment they should inform their line manager. Managers can refer to the DfE 'Cyberbullying: Advice for headteachers and school staff' guidance.

Reporting and recording online safety concerns

- Staff with a concern should always involve the DSL who will be able to make decisions about how and when to escalate a concern.
- DSL will follow the setting safeguarding pathway to address concerns.
- All staff know how to access the settings whistleblowing policy
- If required DSLs will contact:

  The Lincolnshire Safeguarding Team if they have a safeguarding concern about a child and if needed access;

  - the Internet Watch Foundation (IWF) if settings need to report illegal images (child sexual abuse material);
  - the Child Exploitation and Online Protection centre (CEOP) if they are worried about online abuse or the way that someone has been communicating online;
  - the UK Safer Internet Centre Helpline for Professionals or the NSPCC for further information.

The Curriculum

- Spilsby Playgroup is aware that in order for children to live in 'the modern world' technology is important and offers a great many opportunities and avenues for life now and in the future. Our children receive age appropriate, progressive and embedded online safety education throughout the curriculum. E.g. Childnet: 'Keeping young children safe online' and Internet Matters for pre-school and NSPCC online safety

Daily use by staff

Staff make use of technology to support the progress of the children in accordance with the Early Years Foundation Stage. As such each staff member makes use of a Tablet (owned and managed by Spilsby Playgroup). The tablets are used to take pictures of the children and to record observations in order to monitor progress and take learning forward using the online platform of Tapestry.

- Staff are aware that the tablets are purely for the use of recording and supporting children's development and to be used and stored safely in line with GDPR Policy.
- Parents access their own child's Tapestry account via a secure, password protected online account in line with GDPR regulations.
- Parents sign a Tapestry contract to agree that they will not share images on Facebook or other social media source where an image on Tapestry contains other than their own children.

Safety for All

- Spilsby Playgroup is connected to the internet via Spilsby Primary Academy network and as such ensures appropriate filtering and monitoring are in place and the setting
- Access to playgroup's devices is managed and monitored by the management team
- Setting's devices are kept securely and in line with data protection requirements as in our GDPR Policy.
- Physical safety of users has been considered e.g. posture of children/staff when using devices.
- Personal data is managed securely online, in accordance with the statutory requirements of the General Data Protection Regulations (GDPR) and Data Protection legislation.

All staff;

- Are aware that civil, legal or disciplinary action can be taken against staff if they are found to have brought the profession or institution into disrepute.
- Are aware that under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material.
- Are aware of the need to manage their digital reputation, including the appropriateness of information and content that they post online, both professionally and personally.
- Discuss online expectations and behaviour with their friends and colleagues - for example, have they discussed what photos of them can and cannot be shared by their friends on social media.
- Are aware that no matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and/or used without their knowledge or consent.

Links to other Policies

Child Protection and Safeguarding
Prevent Policy
FGM
Staff Code of Conduct

Managing Allegations Against Staff
Whistleblowing
GDPR Policy

.

Appendix 1

Internet Safety Audit (*add name of setting)*……

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**	**Wi-fi enabled** Yes or No?	**Security** settings i.e. passwords, firewalls, screen locks etc..	**Who has access?**
Policies and Procedures -name of policy, or policy in which it is incorporated.	**Subject** • Acceptable use: Yes/No • Staff use of social media Yes/No • GDPR/Data Protection Yes/No • Personal mobile phones / wearable technology		**Policy/Procedure**	**Further action required**	
Approved Apps/websites/online tools.	*List the apps/websites/online tools that you use in your setting with the children* i.e YouTube Kids, CBeebies, Hungry Little Minds.				

How are children supervised when using devices?	Please give details here…
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.
How are devices stored securely when not in use?	Please give details….
How do staff model safe practice when using technology with children?	Please give details…
How is internet safety and use of technology incorporated into the early Years curriculum?	Please give details…
	Add details of information shared with parents to support safe internet use at home.

How is the home learning environment supported?	
Resources to support Internet safety in early years provision.	• **http://internetmatters.org/** • **Online safety guide 0-5 year olds - Internet Matters**