Acceptable Use & Online Safety Policy & Procedure

1. Introduction

At Goldilocks Nursery we recognise that digital technology and the internet offer valuable learning opportunities. We also acknowledge the potential risks to children, staff, and the nursery community. This policy ensures that all digital activity is safe, responsible, and aligned with current UK legislation, EYFS standards, UKCIS guidance, Keeping children Safe in Education guidance and the Online Safety Act.

2. Purpose

This policy aims to:

- Ensure safe and responsible use of digital technology by children, staff, and visitors.
- Safeguard children against inappropriate content, cyberbullying, and privacy breaches.
- Maintain compliance with the Data Protection Act 2018 and EYFS safeguarding requirements.
- Promote digital literacy and safe technology practices.
- Outline reporting procedures for online incidents or concerns.

3. Scope

This policy applies to:

- All staff, including permanent, temporary, and volunteers.
- All children enrolled at the nursery.
- Parents, carers, and visitors using nursery devices or platforms.
- Any digital device or platform used within the nursery setting, including tablets, computers, and online learning platforms.

4. Acceptable Use Guidelines

4.1 Staff and Volunteers

- **Professional Conduct:** Nursery devices must be used for professional purposes. Personal device use should not be used outside of breaks and only in allocated staff areas.
- **Social Media & Digital Communication:** Staff must not share children's images or personal information on personal accounts. Only Famly or nursery email may be used to communicate with parents and are only accessed during working hours.
- **Device Security:** Staff must use strong passwords and lock devices when unattended.
- **Monitoring & Reporting:** Staff are responsible for monitoring children's online activity during supervised sessions. Any concerns should be reported immediately to the Designated Safeguarding Lead (DSL).
- **Training:** Staff will receive regular updates on online safety, GDPR compliance, and safeguarding.

4.2 Children

- **Supervised Access:** Children may only use digital devices authorised and checked by management and DSL under direct adult supervision, appropriate screen time maintained at an acceptable level and is integrated with their learning

- **Age-Appropriate Content:** Only apps, websites, and educational games suitable for early years will be accessible and will be checked prior by the DSL
- **Learning Purpose:** Technology should enhance, not replace, play, creativity, and social interaction.
- **Digital Literacy:** Age-appropriate lessons on online safety will be provided, including age-appropriate simple rules such as "tell an adult if something online upsets you."

4.3 Parents and Carers

- **Awareness & Consent:** Written consent will be obtained before any image, video, or personal data of children is shared digitally.
- **Guidance:** Parents will receive information on online safety at home and guidance on responsible use of technology.
- **Communication:** Parents must use official nursery software such as famly or emails to contact staff, not personal social media.

5. Devices, Software, and Network Management

- **Approved Devices Only:** Only nursery-provided devices may access nursery systems and sensitive data.
- **Software Updates:** All devices will receive regular updates, anti-spyware software and antivirus protection to prevent security breaches.
- **Use Logs:** Access logs will be maintained to track use and identify any inappropriate activity
- **Security of devices:** Devices will be locked away at the end of each day.

6. Safeguarding and Reporting

- **Designated Safeguarding Lead (DSL):** The DSL is responsible for online safety training of staff, children and parent awareness of reporting incident procedures, overseeing online safety and responding to incidents.
- **Incident Reporting:** Any concerns (cyberbullying, inappropriate content, suspicious contact) must be reported immediately to appropriate external contacts.
- **Escalation Procedure:** Serious incidents may be reported to the local safeguarding partnership, police, or other relevant authorities.
- **Child Protection:** Staff must follow safeguarding procedures if online content indicates risk of harm.

7. Data Protection and Privacy

- Personal data (including children's records) will be stored securely and accessed only by authorised personnel.
- Staff must follow GDPR guidelines and confidentiality policy, ensuring minimal data collection, encrypted storage, and secure transfer of information.
- Digital communications must avoid unnecessary sharing of identifiable information about children.

8. Monitoring and Evaluation

- **Regular Reviews:** The policy and online safety procedures will be reviewed at least annually or following significant incidents.
- **Audits:** Devices, logs, and systems will be audited periodically to ensure compliance.
- **Feedback:** Staff, parents, and carers are encouraged to provide feedback on digital safety practices.

9. Roles and Responsibilities

- **Nursery Manager:** Ensures policy implementation, staff training, and reporting compliance.
- **Staff/Volunteers:** Supervise children, enforce guidelines, report concerns.
- **Parents/Carers:** Support the policy, provide consent, reinforce online safety at home.
- **Children:** Follow instructions when using technology and communicate any concerns.

10. Internet Access

- Children do not normally have access to the Internet and never have unsupervised access.
- The designated person ensures children are safeguarded.
- Children are taught stay-safe principles in an age-appropriate way prior to using the internet:
    - Only go online with a grown-up.
    - Be kind online.
    - Keep personal information safe.
    - Only press buttons you understand.
    - Tell a grown-up if something online makes you unhappy.
- Designated persons build children's resilience in relation to online issues and cover topics like safety, appropriate friendships, asking for help, and not keeping secrets in age-appropriate ways.
- If a second-hand computer is purchased or donated, the designated person ensures no inappropriate material is present before children use it.
- Children are not allowed to access social networking sites.
- Staff report any suspicious or offensive material to the DSL who will proceed with the Internet Watch Foundation (www.iwf.org.uk).
- Suspected inappropriate contact by adults is reported to the National Crime Agency's CEOP Centre (www.ceop.police.uk) by the DSL.
- The designated person ensures staff have access to age-appropriate resources to support children online.
- Cyberbullying concerns are discussed with parents and referred to support services like NSPCC (0808 800 5000) or Childline (0800 1111).
- Only authorised staff and parents will have access to the nursery Wi-fi.

11. Email

- Children are not permitted to use email in the setting.
- Parents and staff are not normally permitted to access personal emails on nursery devices and if need be will need permission from management.
- Staff do not access personal or work email while supervising children.
- Personal information is sent securely via encrypted email.

12. Social Media

- Staff manage personal security settings to control information sharing.
- Staff must not accept service users, children, or parents as friends online unless prior relationships were in place before the child attended the setting.
- Staff must not discuss work issues or share information they would not want children, parents, or colleagues to see.
- Staff report any concerns or breaches to the designated person.
- Staff must not display Goldilocks Nursery as their workplace, nor evident that they work in the education sector to others apart from their direct friends and family.

- Personal communication with children or parents must be disclosed to the manager, with agreed boundaries if prior relationships exist.

13. Electronic Learning Journals

- Manager approval and a risk assessment are required before using online learning journals.
- Staff must follow the system guidance at all times.
- Staff must read the Famly policy.
- Staff are not authorised to access famly outside working hours of their shift.

14. Use and/or Distribution of Inappropriate Images

- Staff are aware it is an offence to distribute indecent images.
- Concerns about a colleague's behaviour follow the Child Protection and Safeguarding Children policy.
- Grooming children online is an offence, and concerns must be reported.

15. Further Guidance

- UKCIS Online Safety Guidance for Early Years: gov.uk
- NDNA Online Safety Guidance: ndna.org.uk
- LGfL Digital Safeguarding Resources: viewonline.lgfl.net
- NCSC Cybersecurity Guidance: ncsc.gov.uk
- NSPCC/CEOP Keeping Children Safe Online Training: www.nspcc.org.uk