Little Acorns Montessori

Ascot | Bracknell | Crowthorne

E-Safety (Online Safety) Policy

Applies to all children aged 0–5 | Private Day Nursery | England

1. Document Control

Version	Date	Review Date	Author
1.0	June 2026	June 2027	Jonathan Duffy

This policy must be reviewed annually, after every significant e-safety incident, and whenever relevant legislation or statutory guidance is updated. The Nursery Manager is responsible for ensuring this review takes place.

2. Key Contacts

The following named individuals hold responsibility for e-safety matters at Little Acorns Montessori:

Role	Name	Contact
Designated Officer / Nominated Individual	Jonathan Duffy	All Campuses
Designated Safeguarding Lead (DSL)	Elaine Eastham	Ascot Campus
Designated Safeguarding Lead (DSL)	Agata Payne	Bracknell Campus
Designated Safeguarding Lead (DSL)	Emma Gray	Crowthorne Campus
Deputy Designated Safeguiading Lead (DDSL)	Jessica McGrath/Katy Cooley	Ascot Campus
Deputy Designated Safeguiading Lead (DDSL)	Joanne Broughton	Bracknell Campus
Deputy Designated Safeguiading Lead (DDSL)	Martine Loveridge	Crowthorne Campus
Deputy Designated Safeguiading Lead (DDSL)	Kira King	Crowthorne Campus (in the absence of Emma and Martine)
Manager on Duty	As rostered	All Campuses

3. Policy Statement

Little Acorns Montessori is committed to safeguarding and promoting the welfare of all children in our care. We recognise that the internet and digital technology are an integral part of modern life and that children in the Early Years are increasingly exposed to technology both inside and outside the nursery environment.

This policy sets out our commitment to:

- Protecting all children aged 0–5 from harm arising from the use of, or exposure to, digital technology and online content.
- Ensuring that any use of technology within the nursery supports and enhances the children's learning and development, in line with the EYFS framework.
- Equipping staff with the knowledge, skills and confidence to identify and respond to e-safety risks.
- Providing parents and carers with guidance to support safe digital habits at home.
- Maintaining a safe, secure and proportionate digital infrastructure within all three nursery settings.

This policy applies to all staff (permanent, temporary, agency and volunteers), all children, and all parents and carers accessing Little Acorns Montessori premises or digital platforms. It applies across all three nursery settings in Ascot, Bracknell and Crowthorne.

> *E-safety is a safeguarding matter. Any concern about a child's welfare arising from online activity must be treated with the same urgency as any other safeguarding concern and must be reported to the Designated Safeguarding Lead (DSL) without delay.*

4. Statutory Framework and Legislative Context

This policy is written to fulfil the nursery's obligations under the following legislation and statutory guidance. All referenced documents are current as of the policy review date.

4.1 Early Years Foundation Stage (EYFS) Statutory Framework (DfE, September 2025)

The EYFS Statutory Framework for Group and School-Based Providers (effective 1 September 2025) is mandatory for Little Acorns Montessori as a registered early years provider. The following provisions are directly relevant to this policy:

- **3.1** Section 3 (Safeguarding and Welfare Requirements): Providers must take all necessary steps to keep children safe and well. This includes having a clear policy and procedure in place covering e-safety and the safe use of technology.
- **3.4** The framework requires that providers have in place policies addressing the safe use of electronic devices with imaging and sharing capabilities within the setting.
- **3.19–3.20** The framework requires providers to have a DSL in post, with specific responsibility for safeguarding — including online safety concerns.
- **3.6** Providers must ensure that their safeguarding policies are shared with all staff and parents

4.2 Working Together to Safeguard Children (DfE, December 2023)

All nursery staff must understand their responsibilities to report safeguarding concerns in line with Working Together to Safeguard Children. Online safety concerns may constitute a safeguarding concern. The nursery must ensure that its multi-agency working arrangements align with the Bracknell Forest Safeguarding Board (BFSB) local procedures.

4.3 Keeping Children Safe in Education (KCSIE) (DfE, September 2025)

Whilst KCSIE is statutory guidance for schools and colleges, Little Acorns Montessori voluntarily adopts it as best-practice guidance to inform our e-safety approach. KCSIE 2025 confirms that online safety is a safeguarding matter and that e-safety concerns should be embedded into a setting's child protection policy and procedures. KCSIE 2025 identifies the following as safeguarding harms arising from online activity: content risks (including misinformation, disinformation and conspiracy theories), contact risks, conduct risks, and commerce risks. KCSIE 2025 also references the DfE's Generative AI: Product Safety Expectations guidance (January 2025), which sets out how filtering and monitoring obligations apply to AI-enabled tools used in education settings. Little Acorns Montessori has regard to this guidance when reviewing approved technology and assessing any application that incorporates AI-generated content or AI-assisted features. KCSIE 2025 further references the DfE Cyber Security Standards for Schools and Colleges as a benchmark for digital resilience; the nursery uses these standards as a reference point in its annual filtering and monitoring review.

4.4 The Online Safety Act 2023

The Online Safety Act 2023 received Royal Assent on 26 October 2023. It places legal duties of care on providers of online platforms and services to prevent harmful content being accessed by children. The Act has come into force in stages: illegal content duties came into force in March 2025, and the children's safety duties — including Ofcom's Protection of Children Codes of Practice — came into force on 25 July 2025. These provisions place obligations on platform and service operators, not directly on nursery settings. However, Little Acorns Montessori acknowledges a responsibility to have regard to these provisions when selecting, approving or recommending any digital platform for use by children or families. Before any platform is introduced for use with children or recommended to parents and carers, the Nursery Manager will carry out a proportionate check to satisfy themselves that the platform has met its obligations under the Act, including Ofcom's children's access assessment and content risk assessment requirements where applicable.

4.5 The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)

The nursery must process all personal data, including photographs and video recordings of children, in accordance with the Data Protection Act 2018 and the UK GDPR. Consent must be obtained before any images of children are taken or shared, and data must be stored securely.

4.6 The Childcare Act 2006

The safeguarding and welfare requirements set out in EYFS Section 3 are given legal force by Regulations made under Section 39(1)(b) of the Childcare Act 2006. Non-compliance with these requirements may result in regulatory action by Ofsted.

4.7 The Children Act 1989 and 2004

The nursery's overriding duty is to promote and safeguard the welfare of children. Section 47 of the Children Act 1989 places a duty on local authorities to investigate concerns about children at risk of significant harm. Any e-safety incident that gives rise to a child protection concern must be referred in accordance with these provisions.

5. Scope of This Policy

This policy covers e-safety risks and responsibilities across four key domains:

- Content risks — exposure to age-inappropriate, harmful or illegal online content.
- Contact risks — unwanted or inappropriate contact with adults or peers through digital platforms.
- Conduct risks — children's own online behaviour, including the sharing of images.
- Commerce risks — exposure to inappropriate advertising, in-app purchases, or online manipulation.

The policy applies to the use of all internet-connected technology, including but not limited to:

- Desktop computers, laptops and tablets used within the nursery.
- Interactive whiteboards and smart screens.
- Staff smartphones and personal devices brought onto nursery premises.
- The nursery's website, parent communication apps, and social media accounts.
- Any technology used by children as part of their learning and play activities.

6. Risk Assessment

The Nursery Manager and DSL must undertake a written e-safety risk assessment at least annually. The risk assessment must:

- Identify the specific e-safety risks present across all three nursery sites.
- Assess the likelihood and potential impact of each risk on children in the setting.
- Document the controls and mitigations in place to address each risk.
- Be reviewed following any significant e-safety incident or change in the nursery's digital infrastructure.

The risk assessment must give consideration to risks arising from:

- Children's use of nursery devices and technology during the session.
- Staff use of personal devices on nursery premises.
- The nursery's use of apps, platforms and communication tools that involve the processing of children's images or data.
- Parents' and visitors' use of smartphones and devices on nursery premises.
- Children arriving at nursery having been exposed to harmful online content at home.

7. Safe Use of Technology with Children

7.1 Approved Technology and Content

- Only nursery-approved devices may be used with children during sessions.
- All devices used with children must have appropriate content-filtering software and up-to-date anti-virus protection installed.
- Staff must only use pre-approved, age-appropriate applications and online content with children.

- A register of approved apps and platforms must be maintained by the Nursery Manager and reviewed annually.
- Before introducing any new digital resource to children, staff must obtain approval from the Nursery Manager.
- Before approving any application or platform for use with children or for recommendation to families, the Nursery Manager must consider whether the application incorporates AI-generated content or AI-assisted features and, if so, assess it against the DfE's Generative AI: Product Safety Expectations guidance. The Nursery Manager must also carry out a proportionate check that any platform recommended to families meets its obligations under the Online Safety Act 2023, including Ofcom's Protection of Children Codes where applicable.

7.2 Supervision of Children's Technology Use

- Children must be supervised by a member of staff at all times when using any digital device.
- Staff must not leave children unattended with internet-connected devices.
- Staff must monitor the content children are accessing and intervene immediately if inappropriate content is encountered.
- Any accidental exposure to inappropriate content must be reported to the DSL on the same day.

7.3 Online Safety Education for Children

- Age-appropriate online safety education should be incorporated into the nursery's curriculum in line with EYFS areas of learning, particularly Communication and Language, and Understanding the World.
- Stories, activities and discussions about safe technology use should be woven into everyday practice.
- Staff should model positive, safe and responsible technology use in the presence of children at all times.

8. Staff: Acceptable Use and Conduct

8.1 Personal Devices

- Staff must not use personal mobile phones or devices in children's rooms or when directly responsible for children's supervision.
- Personal devices must be stored securely out of reach of children when not in use.
- Staff must never use personal devices to photograph or film children.
- Any emergency use of a personal device must be reported to the Nursery Manager.

8.2 Nursery Devices

- Staff must only use nursery-owned devices for the purposes of their professional duties.
- Staff must not access personal social media accounts, personal email, or non-work websites on nursery devices.
- Staff must log out of all systems at the end of their session and must not share passwords.

- Any suspected breach of the nursery's IT security (including loss or theft of a device) must be reported to the Nursery Manager and DSL immediately.

8.3 Photography and Images of Children

- Photography and recording of children is only permitted using nursery-owned devices.
- Parental/carer consent must be obtained before any images of children are taken, in accordance with the nursery's Photography and Images Policy.
- Images must be stored securely on the nursery's approved platform and must not be transferred to personal devices or personal cloud storage.
- Images must not be shared on personal social media accounts under any circumstances.
- All images must be deleted from devices once they have been securely transferred and backed up, in accordance with the nursery's data retention schedule.

8.4 Social Media

- Staff must not post images or identifying information about children or their families on any personal social media platform.
- Staff must not make any comment about the nursery, its children or its families on personal social media that could be considered unprofessional, discriminatory or that could bring the nursery into disrepute.
- Staff must not accept parent/carer social media connection requests on personal accounts.
- Staff should be aware that a breach of these requirements may constitute a safeguarding concern and will be addressed under the nursery's disciplinary procedures.

8.5 Nursery's Official Social Media and Digital Platforms

- Only the Nursery Manager or a designated member of staff with written authorisation may post content on the nursery's official social media accounts or website.
- No images of identifiable children must be posted publicly without specific written parental consent.
- The nursery's official accounts must only be used for professional purposes.

8.6 Training Requirements

- All staff must complete e-safety training as part of their induction, prior to working independently with children.
- All staff must refresh their e-safety training at least every two years, or sooner if required following an incident or a significant change in legislation or guidance.
- The DSL must receive more in-depth e-safety training to enable them to provide support and guidance to colleagues.
- Training records must be maintained by the Nursery Manager and made available for inspection.

8.7 Reporting concerns about colleagues

- Any member of staff who has a concern that a colleague may be behaving in a way that puts children at risk online — including through inappropriate use of devices,

sharing of images, or failure to follow this policy — must report that concern immediately to the DSL or Nursery Manager. Where a member of staff does not feel able to raise the concern internally, or where the concern relates to the Nursery Manager or DSL themselves, they should refer to the nursery's Whistleblowing Policy for guidance on external reporting routes. The EYFS Statutory Framework (September 2025) explicitly requires all providers to have whistleblowing procedures in place for all staff, including students and volunteers.

9. Parents, Carers and Visitors

9.1 Mobile Phones and Devices on Nursery Premises

- Parents and carers are required to limit their use of mobile phones on nursery premises, particularly in areas where children are present.
- Photography and filming of children by parents or visitors is not permitted within the nursery without prior written consent from all relevant parties and approval from the Nursery Manager.
- All visitors to the nursery must follow the nursery's mobile phone policy, which will be communicated upon arrival.

9.2 Parent Communication Platforms

- The nursery uses a parent-facing communication platform (such as a nursery app) to share updates, observations and information about children.
- Parents and carers must use this platform responsibly and must not share access with third parties.
- The nursery will inform parents of the platform's data handling practices and obtain appropriate consent.

9.3 E-Safety Guidance for Families

- The nursery should provide parents and carers with regular e-safety information, including guidance on age-appropriate screen time and online safety at home.
- E-safety resources should be made available via the nursery noticeboard, newsletter, and parent platform.
- Parents who have concerns about a child's online activity at home are encouraged to raise these with the DSL.

10. Procedures for Managing E-Safety Incidents

All e-safety concerns must be dealt with promptly and in accordance with the following procedure. These steps are chronological and must be followed in order.

Step 1 — Immediate Response

- Any member of staff who identifies, witnesses, or suspects an e-safety incident must act immediately to ensure the safety of any child involved.
- Where a child has been exposed to harmful content, the device must be closed or removed from the child's access without further interaction with the content.

- Where possible, the member of staff must preserve the evidence (for example, by noting the URL, taking a note of the content seen, or preserving the device without further use) before closing the content.
- The member of staff must not attempt to investigate the matter themselves, access further content, or take screenshots using a personal device.

Step 2 — Report to the DSL

- The member of staff must report the concern to the DSL (or Deputy DSL in the DSL's absence) on the same day, without delay.
- The report must be made verbally in the first instance, followed by a written record (see Section 11).
- If the DSL is not available and the concern is urgent, the Nursery Manager must be informed immediately.

Step 3 — Initial Assessment by the DSL

- The DSL must assess the concern and determine whether it constitutes a safeguarding risk to the child.
- The DSL must consider whether the concern requires immediate referral to children's social care (Bracknell Forest Children's Services), the police, or another external agency.
- The DSL must follow the Bracknell Forest Safeguarding Board's local procedures when making any referral.
- If it is not immediately clear whether a referral is required, the DSL should seek advice from the BFSB duty team without necessarily identifying the child.

Step 4 — Parental Notification

- Parents and carers must be notified of any e-safety incident involving their child, unless doing so would place the child at increased risk of harm.
- The DSL must make the decision on whether, when, and how parents are informed.
- If a referral to children's social care has been made, the DSL must seek guidance from the relevant social worker before contacting parents.

Step 5 — Reporting to External Agencies

- Illegal online content (including child sexual abuse material) must be reported to the Internet Watch Foundation (IWF) at www.iwf.org.uk.
- Online grooming, exploitation or abuse must be reported to the National Crime Agency's CEOP Command at www.ceop.police.uk.
- Where a crime has been committed or where a child is at immediate risk, the nursery must contact the police (999 for emergencies; 101 for non-emergencies).
- The DSL must refer to the BFSB guidance on thresholds and escalation when determining the appropriate referral pathway.

Step 6 — Review and Learning

- Following the resolution of any e-safety incident, the DSL must conduct a review to identify any learning or changes to practice required.

- Where appropriate, the nursery's e-safety policy, risk assessment, or staff training programme should be updated.
- The DSL must consider whether any themes or patterns of incidents require a more systemic response.

11. Reporting and Recording

Accurate and timely recording is essential. The following requirements apply to all e-safety incidents:

- All e-safety incidents must be recorded on the nursery's E-Safety Incident Log on the same day as the incident occurs, or as soon as practicable thereafter.
- The written record must be completed by the member of staff who first identified the concern, in conjunction with the DSL.

The record must include, as a minimum:

  - Date and time of the incident.
  - Name of the child(ren) involved (where applicable).
  - Name of the member of staff who identified or was involved in the incident.
  - A factual description of what occurred, including the nature of any content seen.
  - Immediate actions taken.
  - Name of the DSL informed and the date and time they were informed.
  - Any external referrals made, including the agency contacted, date, and reference number.
  - Actions agreed and outcome.
  - Signature of the DSL.

- All e-safety incident records are classified as confidential child protection records.
- Records must be stored securely in the nursery's locked child protection filing system (physical) and/or in the nursery's password-protected secure case management system (digital).
- Access to e-safety incident records must be restricted to the Nursery Manager, DSL, Deputy DSL, and any external agencies or inspectors with a lawful basis for access.
- Records must be retained in accordance with the nursery's data retention policy and UK GDPR obligations. Child protection records must be retained for a minimum period in line with the BFSB guidance, regardless of when the child leaves the nursery.
- In the event of an Ofsted inspection, e-safety incident records must be made available to inspectors upon request.

12. Roles and Responsibilities

Role	Key Responsibilities
Nursery Manager	• Hold overall accountability for the e-safety policy and its implementation.

	• Ensure the policy is reviewed annually and following any significant incident. • Ensure all staff receive appropriate e-safety training as part of induction and ongoing CPD. • Report e-safety concerns to Ofsted as required under the EYFS. • Maintain up-to-date knowledge of local safeguarding arrangements via the Bracknell Forest Safeguarding Board (BFSB).
Designated Safeguarding Lead (DSL)	• Take lead responsibility for all e-safety concerns and referrals. • Liaise with the Bracknell Forest Safeguarding Board and relevant statutory agencies. • Maintain the e-safety incidents log and ensure records are stored securely. • Provide e-safety guidance and support to all staff. • Stay updated on emerging online risks and update procedures accordingly. • Report any e-safety concern involving a child to children's social care where appropriate.
Deputy DSL	• Support the DSL in all e-safety responsibilities. • Act as the lead for e-safety in the absence of the DSL. • Maintain sufficient training and competency to fulfil the DSL role if required.
All Staff	• Complete e-safety training at induction and at least every two years thereafter. • Model safe, responsible and positive use of technology at all times. • Report any e-safety concern to the DSL immediately. • Adhere to the nursery's acceptable use policy for all devices. • Never share images or information about children on personal devices or personal social media. • Challenge and report any unsafe online behaviour they observe.
Parents and Carers	• Read and acknowledge the nursery's acceptable use agreement upon enrolment. • Notify the nursery of any e-safety concerns arising at home that may affect the child. • Follow the nursery's mobile phone and photography policy on the premises. • Engage with e-safety guidance and resources provided by the nursery.

13. Filtering and Monitoring

Little Acorns Montessori must maintain appropriate technical safeguards on all internet-connected devices and networks. The following minimum standards apply:

- All internet-connected devices used in the nursery must be protected by up-to-date anti-virus and anti-malware software.
- Content filtering must be in place on all nursery devices to prevent access to age-inappropriate or harmful websites. The filtering system must be reviewed at least annually and after any significant change to the nursery's IT infrastructure.
- Strong, unique passwords must be used for all nursery systems and devices. Passwords must not be shared between staff members. Default passwords must be changed upon initial setup.
- The nursery's Wi-Fi network must be password-protected. Guest access, where provided, must be on a segregated network that does not allow access to the nursery's internal systems.
- The DSL should be familiar with the nursery's filtering and monitoring arrangements and should be able to describe them to an Ofsted inspector.
- Where the nursery uses cloud-based storage or communication platforms, these must comply with UK GDPR and must be hosted by a provider with appropriate data security certifications.
- When reviewing filtering and monitoring arrangements, the Nursery Manager and DSL must consider whether any approved applications incorporate generative AI features, and must satisfy themselves that appropriate safeguards are in place in respect of AI-generated content accessible to children, having regard to the DfE's Generative AI: Product Safety Expectations guidance (January 2025).
- The nursery will use the DfE Cyber Security Standards for Schools and Colleges as a reference benchmark when reviewing its digital infrastructure, including arrangements for multi-factor authentication on administrative systems, regular software patching, and secure Wi-Fi configuration. This review must take place at least annually and findings must be recorded.

14. Linked Policies and Procedures

This policy must be read in conjunction with the following nursery policies:

- Child Protection and Safeguarding Policy
- Photography and Images Policy
- Data Protection and UK GDPR Policy
- Social Media Policy
- Acceptable Use Policy (Staff)
- Mobile Phone and Personal Device Policy
- Whistleblowing Policy
- Behaviour Management Policy

Staff must be familiar with all linked policies. Updated versions of all policies are held in the nursery's policy folder and on the nursery's staff digital platform.

15. Breaches of This Policy

Any breach of this policy by a member of staff will be taken seriously and may result in disciplinary action up to and including dismissal.

A breach that constitutes a safeguarding concern — for example, inappropriate sharing of images of children, grooming behaviour, or failure to report an e-safety incident — must be

referred to the DSL immediately and may result in referral to the Disclosure and Barring Service (DBS) and/or the police.

Any breach of this policy by a parent or visitor will be addressed by the Nursery Manager and may result in restricted access to the nursery.

16. Policy Review

This policy must be reviewed:

- Annually, as a minimum, by the Nursery Manager and DSL.
- Following any significant e-safety incident within the nursery.
- Following any material change to relevant legislation or statutory guidance (including updates to the EYFS framework, KCSIE, or the Online Safety Act 2023).
- Following any significant change to the nursery's digital infrastructure or platforms.

The review date is recorded in the Document Control Table in Section 1. All staff must be informed of any substantive changes to this policy.

This policy was written in accordance with the EYFS Statutory Framework for Group and School-Based Providers (effective 1 September 2025), Working Together to Safeguard Children (December 2023), and the Online Safety Act 2023. Little Acorns Montessori is registered with Ofsted and operates under the Bracknell Forest Safeguarding Board local multi-agency safeguarding arrangements.

Policy Approval

Role	Name	Date
Owner/Director	Jonathan Duffy	June 2026