

Bloom Childcare

Photography, Images, Social Media & Acceptable Use of Technology Policy

Document Register Detail			
Document Name:	Photography, Images, Social Media & Acceptable Use of Technology Policy		
Document ID:	B0020	Issue Date:	1 st October 2026
Version:	V2	Review Date:	1 st October 2027
Responsible Person:	Mark Johnson - MD	Status:	Live

1. Policy Statement

Bloom Childcare is committed to protecting the privacy, dignity and safety of every child in our care and to promoting safe, responsible use of technology across all settings. We recognise that photographs and videos of children carry significant safeguarding implications, that the growth of social media creates additional risks in relation to image sharing, and that all technology used within the setting must be controlled and used appropriately.

This policy sets out how Bloom Childcare captures, stores, uses and shares images of children and staff; how it governs the use of all technology - including nursery devices, personal devices, online platforms and digital systems; and how it manages staff conduct in relation to social media. Our approach is grounded in the legal rights of children and families, the requirements of the EYFS Statutory Framework for group and school-based providers, UK GDPR and the Data Protection Act 2018.

No image of a child will ever be taken, shared or published without appropriate consent. No technology will be used in a way that could place a child, family or colleague at risk of harm, embarrassment or exploitation.

2. Scope

This policy applies to:

- All Bloom Childcare employees, including permanent, temporary and agency staff
- Volunteers, students and apprentices
- Contractors and visitors on site

- Parents, carers and family members attending setting events
- All devices used at or for the setting, whether setting-owned or personal
- All platforms and channels through which images or content relating to Bloom Childcare or its children may be shared, including social media, email and messaging apps

3. Relevant Legislation and Guidance

Legislation / Guidance	Description	Relevance to This Policy
UK General Data Protection Regulation (UK GDPR)	The primary framework governing how personal data - including images of identifiable individuals - is collected, stored and used.	Images of children are personal data. Consent and legitimate purpose must be established before capture or use.
Data Protection Act 2018	UK domestic legislation supplementing UK GDPR, including special provisions for children's data.	Children warrant enhanced protection; their images and digital data must be handled with extra care.
EYFS Statutory Framework 2026	Sets safeguarding and welfare requirements for early years providers, including use of mobile technology.	Providers must have a policy on the use of mobile phones, cameras and other electronic devices with imaging and sharing capabilities in the setting (§3.4), DfE screen use guidance for early years settings
Children Act 1989 & 2004	Establishes the paramount importance of children's welfare and the duty to safeguard.	Underpins all decisions about image use and technology conduct in relation to children.
Human Rights Act 1998	Article 8 – Right to respect for private and family life.	Children and families have a right to privacy; image capture and data use must not infringe this right.
Ofsted Education Inspection Framework 2023	Sets out how Ofsted judges the effectiveness of safeguarding arrangements.	Inspectors will review the setting's policy and practice around photography, technology and social media.
Online Safety Act 2023	Imposes duties on service providers to protect users, particularly children, from online harms.	Reinforces the setting's duty to supervise and support children's safe use of digital technology.

4. Definitions

Term	Definition
------	------------

Images	Photographs, video footage, audio-visual recordings or screen captures in which a child or member of staff is identifiable.
Personal Device	Any technological device; film cameras, mobile phone, smartphone, tablet, laptop, camera, webcam, smart watch or recording device that is privately owned and not issued by Bloom Childcare.
Setting Device	Any device owned by, registered to and managed by Bloom Childcare, including tablets, cameras, computers and nursery management systems.
Social Media	Any internet-based platform or application that enables users to create and share content or participate in social networking, including (but not exclusively) Facebook, Instagram, TikTok, X (Twitter), Snapchat, WhatsApp, LinkedIn, BlueskySocial and YouTube.
Acceptable Use	The use of technology in a way that is lawful, professional, purposeful, safe and consistent with Bloom Childcare's policies and values.
E-Safety	The safe and responsible use of digital technology, including the internet, social media, online platforms and all electronic devices.
Consent	A freely given, specific, informed and unambiguous indication of agreement, given by those holding parental responsibility for a child under 13, or by an adult subject themselves.
Parental Responsibility	As defined in the Children Act 1989 - all rights, duties, powers and responsibilities a parent or guardian has in relation to a child.
Data Breach	Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data including images or digital records.
DSL	Designated Safeguarding Lead - the nominated person responsible for safeguarding and child protection at the setting.

5. Roles and Responsibilities

5.1 Managing Director / Setting Manager

- Ensure this policy is implemented, reviewed and communicated to all staff

5.1 Area Manager

- Take lead responsibility for ensuring that all setting devices are appropriately managed, secured and monitored
- Take lead responsibility for any data breaches involving images or digital records of children
- Act as the point of escalation for any concerns relating to inappropriate photography, technology use or social media conduct
- Oversee Setting Managers to ensure all staff complete required training on e-safety and acceptable use

5.2 Setting Managers

- Maintain and review consent list/register
- Take responsibility for ensuring that all setting devices are appropriately managed, secured and monitored
- Ensure this policy is implemented, reviewed and communicated to all staff at their setting
- Ensure staff mobile phones are kept in designated storage area during work hours
- Review parental consent for their setting regularly
- Ensure that all setting devices are appropriately used, secured and monitored
- Ensure that images are deleted from the device after successful transfer to the secure storage system
- Report any data breaches involving images or digital records of children
- Ensure all staff complete required training on e-safety and acceptable use / induction

5.3 All Staff

- Adhere strictly to this policy at all times, including during off-site activities and events
- Use all setting technology - including tablets, computers, cameras and software - solely for work-related purposes that support children's learning, development and safeguarding
- Never use a personal device to photograph, film or record children in the setting
- Never share, post or publish images of children on personal social media accounts
- Complete all required training on online safety, data protection and e-safety procedures as required
- Report any concerns about a colleague's use of devices or social media to the Setting Manager immediately

5.4 Designated Safeguarding Lead (DSL)

- Act as the first point of contact for any concerns relating to inappropriate image capture, online safety incidents or misuse of technology
- Escalate concerns to the LADO or Police where a child may be at risk
- Maintain records of all technology and e-safety concerns and actions taken

5.5 Parents and Carers

- Complete and sign the image consent (online registration form) on or before the child's start date
- Inform Bloom Childcare immediately of any change in consent preferences
- Respect the privacy of other children at the setting - do not photograph or film other children during events

6. Acceptable Use of Technology

All staff are expected to use technology within the setting in a manner that is lawful, professional and consistent with Bloom Childcare's values and safeguarding obligations. The following requirements apply to all use of technology at the setting:

- All technology - including nursery tablets, computers, cameras and software - must be used solely for work-related purposes that support children's learning, development and safeguarding
- Staff must not access, download or store any content that is illegal, offensive, discriminatory, political, sexually explicit or otherwise inappropriate on any setting device or system
- Staff must not use setting devices for personal activities, personal social media, personal shopping, gaming or any purpose unrelated to their professional duties
- All passwords and login credentials for setting systems must be kept confidential and must not be shared with colleagues, parents, children or third parties
- Staff must lock a device or system when leaving it unattended
- Any technical fault, suspected security breach or loss or theft of a setting device must be reported to the Setting Manager immediately

Monitoring: All device usage within the setting may be monitored and audited by management to ensure compliance with safeguarding protocols and this policy. Staff should have no expectation of privacy when using setting-owned devices or networks.

7. Children's Screen Use

Screen use is purposeful, developmentally appropriate and supervised; does not routinely replace active play, physical activity, social interaction, communication, outdoor experiences or sleep/rest; and follows the DfE screen-use guidance. At Bloom, screen use is not part of the formal curriculum.

8. Consent for Photography and Images

Bloom Childcare obtains written consent from those holding parental responsibility before capturing or using any image of a child. Consent is sought through the online Registration Form and covers the following specific purposes:

- Learning journey and progress documentation
- Display within the setting (e.g. on noticeboards or learning journey displays)
- Saving to Bloom Childcare's secure digital platforms (Google/iConnect/Noodle)
- Marketing and promotional materials (website, printed brochures, local press)
- Social media posts on Bloom Childcare's official, managed accounts
- Any other appropriate medium

A further, distinct purpose applies specifically to Educational Visits (EV trips): with prior written agreement (obtained at registration or via the trip-specific consent form), the Lead Practitioner may photograph a child on the company smartphone immediately before departure, for use solely in helping staff or the emergency services identify the child during a

trip emergency. This purpose is recorded separately from the purposes above, and the images are never transferred to the secure storage system - see the Educational Visits (EV) Policy (B0025) for the full procedure and the applicable retention rule.

Consent for each purpose is requested and recorded separately. Parents may grant consent for some purposes and not others. All consent is freely given and may be withdrawn at any time by written notification to the Setting Manager.

Important: Withdrawal of consent will be acted upon promptly. Images will be removed from digital platforms and future publications. It is not always possible to recall images already printed or distributed to third parties - parents will be informed of this limitation at the point of withdrawal.

Where a child has a protection plan, court order or other safeguarding measure in place that restricts disclosure of their whereabouts, no images of that child will be taken or used for any external purpose. The Setting Manager will ensure this is communicated to relevant staff on a need-to-know basis.

9. Use of Setting Devices

Bloom Childcare uses designated setting devices (tablets, phones or cameras) for capturing images of children. These devices are managed, secured and owned by the setting.

- Setting devices must not leave the premises unless specifically authorised by the Setting Manager for an off-site activity
- Images captured on setting devices are stored only in designated, password-protected, setting-controlled locations (e.g. secure learning journey platform or passworded server)
- Images are not stored in personal cloud storage accounts or personal email accounts
- Setting devices are not used for personal social media, personal email or any purpose unrelated to the child's care and development
- Images are deleted from the device after successful transfer to the secure storage system
- Setting devices are password-protected and must not be accessed by children, parents or visitors
- Only setting-approved devices may be used for capturing observations or engaging with digital learning content

10. Personal Devices (Mobile Phones and Cameras)

In line with EYFS, Bloom Childcare operates a strict personal device policy to safeguard children.

Smart glasses and wearable recording devices: camera-enabled smart glasses or other wearable recording devices (for example, Meta Ray-Ban glasses or similar eyewear capable of photography, video or audio recording) must not be worn anywhere on Bloom Childcare premises or grounds, by anyone, under any circumstances. Unlike a mobile phone, these devices can record without any visible indication that they are doing so, which the setting

considers an unacceptable safeguarding risk. Any person wearing such a device on arrival will be asked to remove it and store it before entering any area of the setting.

10.1 Staff

- Personal mobile phones and cameras must be kept in designated storage (e.g. staff lockers or the office) during working hours and must not be brought into childcare areas
- Staff must not use personal devices to photograph, film, record or screen-capture any child at the setting at any time, or the setting itself (inside or outside) including during outings and events
- Staff must not contact parents or carers via personal devices - all communication must use setting-managed channels and normally via the Setting Manager
- In an emergency where a personal device must be used, the Setting Manager must be informed immediately afterwards and the circumstance reported to senior management
- **Staff must not use personal devices to take photos, videos or audio recordings of any child under any circumstances**

10.2 Visitors and Contractors

- Visitors and contractors are informed of this policy on arrival and before work commences
- Personal devices must not be used in areas where children are present without the explicit permission of the Setting Manager
- Any visitor who refuses to comply may be asked to leave the premises

10.3 Parents and Carers

- Parents' and carers' personal mobile phones and other personal devices must not be used to take photographs or video recordings, or to make video calls (including FaceTime or similar), anywhere on Bloom Childcare premises or grounds
- This applies even where only the parent's or carer's own child would be included in the image or call, as other children may be visible or audible in the background
- The setting will remind parents and carers of this requirement at events and via setting communications

11. Digital Images and Media

The following requirements apply to all images and recordings of children, regardless of the device or platform used:

- All images or recordings of children must be used only in accordance with this policy and with written parental consent (online registration form or updated email)
- Images or videos of children must never be shared via personal devices, personal email accounts or personal social media platforms

- Images must not contain metadata (geo-tagging) that could disclose the setting's location or a child's home address - all images are stripped of metadata before external use
- No child's full name will be used alongside an image in any external communication or publication
- Images shared via the setting's secure digital platform must only be accessible by authorised staff
- USB drives and unencrypted portable media must not be used to store children's images

12. Social Media

12.1 Official Bloom Childcare Social Media

Bloom Childcare maintains official social media accounts for the purpose of communicating with the community and marketing. The following standards apply:

- Only an authorised designee may post content on behalf of Bloom Childcare
- Images of children will only be posted where specific consent for social media use has been obtained
- Staff must only post content relating to Bloom on official company social media accounts

12.2 Staff Personal Social Media

Bloom Childcare has legitimate expectations of staff conduct on personal social media, including outside working hours or at Bloom staff social events, where such conduct could affect the setting, its children or the business' reputation.

- Staff must not post, share, comment on or discuss any image of a child in the setting's care on personal social media, regardless of whether consent has been given for other purposes
- Staff must not post content that could identify the setting, a family or a child in a context that brings the setting into disrepute
- Staff must not use social media to contact, or respond to contact from, parents or carers in relation to their child's care
- Staff must not post negative, derogatory or confidential comments about children, families, colleagues or the business on any platform
- Staff who are unsure whether a post is appropriate should not post it - they should seek guidance from the Setting Manager

Note: Breaches of the social media requirements in this policy will be investigated under Bloom Childcare's Disciplinary Procedure. Depending on the severity, a breach could constitute Gross Misconduct, potentially resulting in dismissal without notice. Staff are reminded that this applies to personal as well as professional accounts.

13. Online Safety and Supervision of Children

Where children use digital devices or engage with any form of technology within the setting, staff have an active duty to supervise and safeguard them. The following requirements apply:

- Staff must actively supervise children at all times when they are using digital devices, online platforms or any technology-based learning resource
- Children must not be given access to the device, internet, social media or any platform or content that has not been pre-approved by the Setting Manager
- Staff must report any concerns regarding a child's online activity, or any inappropriate content encountered by a child, to the DSL immediately
- Staff will support children in understanding how to use technology safely and responsibly, in a manner appropriate to their age and stage of development
- Any online safety incident - including a child accessing inappropriate content, online grooming or cyberbullying - must be recorded and reported in line with Bloom Childcare's Child Protection and Safeguarding Policy

Bloom Childcare will ensure that any internet connectivity available to children uses appropriate content filtering.

14. Data Protection and Confidentiality

All images and digital information relating to children, families and colleagues are classified as personal data under UK GDPR and must be handled accordingly:

- Staff must not share any personal data, photos or information about children, families or colleagues without proper authorisation and a legitimate purpose
- Staff must follow Bloom Childcare's Confidentiality Policy & Data Protection (B0033) when storing or sharing any digital information
- Images are retained for the duration of the child's placement plus a period consistent with Bloom Childcare's Data Retention Policy, then securely deleted
- Upon a child leaving the setting, their learning journey (including images) will be provided to the parent or carer if they so wish; images held on setting systems will then be securely deleted within 30 days unless a longer period is required for legal or regulatory reasons
- Any external sharing of images (e.g. with local press or for award agencies) requires specific consent and is documented
- Photographs taken for EV trip emergency identification purposes (B0025) follow a separate, shorter retention rule: they are deleted from the device immediately upon the group's successful return to the setting, rather than the general retention period above

15. Reporting a Data Breach Involving Images or Digital Data

Any actual or suspected unauthorised disclosure, loss or misuse of children's images or digital data must be reported immediately to the Setting Manager, who will:

- Assess the breach against the ICO's threshold for mandatory reporting
- Where required, notify the ICO within 72 hours of becoming aware of the breach
- Inform affected parents or carers where there is a high risk to their rights and freedoms

- Document the breach, the assessment and all actions taken in the Setting's Data Breach Log

16. Concerns and Safeguarding

Any concern that a person - whether a member of staff, visitor, parent or contractor - has taken or shared an inappropriate image of a child, or has used technology inappropriately in relation to a child, must be reported to the DSL immediately. This includes:

- Photographs or videos taken without consent or in a covert manner
- Images that appear to be sexual, exploitative or inappropriate in any way
- Images of a child shared on social media without the setting's knowledge or parental consent
- Any situation where a child has been photographed in a state of undress or in a manner that could cause embarrassment or harm
- Any online safety incident involving a child, including exposure to harmful content, grooming or cyberbullying

Safeguarding Alert: Where a device is involved in a concern, evidence must not be tampered with or deleted. Staff should not handle the device and should preserve it for investigation. The Police may require the device as evidence. Contact the DSL immediately.

17. Professional Conduct and Disciplinary Consequences

Breaching any element of this policy is a serious matter. All staff acknowledge, through completing Induction training, that they have read, understood and agreed to comply with this policy.

Breaches of this policy will be investigated under Bloom Childcare's Disciplinary Procedure. Depending on the nature and severity of the breach, this may result in:

- A formal verbal or written warning
- A final written warning
- Dismissal with notice
- Summary dismissal (Gross Misconduct) - applicable particularly to breaches involving inappropriate photography or sharing of children's images
- Referral to the Disclosure and Barring Service (DBS) and/or relevant regulatory bodies
- Referral to the Police where a criminal offence may have been committed

18. Staff Training and Awareness

All staff receive induction training that includes the requirements of this policy. Training covers:

- UK GDPR obligations and the legal basis for consent
- Correct use of setting devices and the prohibition on personal devices in childcare areas
- Appropriate and inappropriate use of social media
- E-safety principles and the supervision of children using technology
- How to recognise and respond to concerns about inappropriate photography or image sharing
- Data protection and confidentiality obligations

19. Monitoring and Review

The Setting Manager is responsible for monitoring compliance with this policy and will:

- Review the Consent Register at least annually and update where circumstances have changed
- Conduct periodic spot-checks to ensure setting devices are used appropriately and securely
- Monitor and audit device usage to ensure compliance with safeguarding protocols
- Log any reported concerns, breaches or incidents and record the actions taken

This policy will be formally reviewed annually, or sooner following any significant incident, change in legislation or updated regulatory guidance. All revisions will be approved by the Managing Director before the updated version takes effect.

20. Policy Sign-off and Authorisation

DECLARATION			
Role	Name	Signature	Date
Managing Director / Duty Holder	Mark Johnson		1 st October 2026