Acceptable Use Policy

What's the Goal of the Policy?

At Brize Norton Village Preschool, safeguarding children includes protecting them when technology, electronic devices and online services are being used.

Technology can provide valuable opportunities to support children's learning, communication and development. However, its use must always be purposeful, age appropriate, closely supervised and balanced with children's need for active, physical, social and real-world experiences.

We recognise online safety as an integral part of safeguarding and understand that our responsibility extends to the way staff use technology, how information about children is stored and shared, how images are captured and used, and how we support children to begin developing safe and healthy relationships with technology.

Our aim is to:

- keep children safe when accessing technology;
- ensure technology is used appropriately and purposefully;
- protect children's personal information and images;
- establish clear professional boundaries for staff;
- ensure preschool devices and accounts are secure;
- reduce the risk of inappropriate, harmful or illegal content being accessed;
- ensure staff understand how to identify, record and report online safety concerns;
- support children to develop age-appropriate understanding of online safety;
- support parents and carers to understand how we promote online safety; and
- ensure any loss, theft, misuse or data breach involving nursery technology is responded to appropriately.

Online safety is everyone's responsibility. The Designated Safeguarding Lead (DSL) takes lead responsibility for online safeguarding concerns.

What Does Acceptable Use Look Like?

Preschool Devices - Only devices authorised by Brize Norton Village Preschool may be used to photograph children, access children's records or undertake other activities involving children's personal information.

This may include:

- tablets/iPads;
- nursery mobile phones;
- laptops;
- other approved digital equipment.

All preschool devices must:

- be password/passcode protected;
- have automatic screen locking enabled where possible;
- be kept securely when not in use;
- only contain applications authorised by the preschool
- have appropriate security and software updates maintained;
- use appropriate filtering and security controls where internet access is available;
- only connect to authorised and secure networks;

- only be accessed by authorised individuals;
- be used in accordance with data protection requirements; and
- never be left unattended where children or unauthorised individuals could access confidential information.

Passwords and passcodes must not be shared with children, parents or unauthorised individuals.

Staff must immediately report any suspected unauthorised access to a preschool device or account.

Taking and Storing Photographs and Videos

Photographs and videos of children may only be taken using preschool-authorised devices and for legitimate purposes.

Staff must:

- check that appropriate parental permissions are in place;
- consider children's dignity when taking photographs;
- never take photographs or videos of children in circumstances that could be considered inappropriate or intrusive;
- never use a personal device to photograph or record children;
- ensure images are transferred/stored using approved systems;
- not retain images unnecessarily;
- never transfer children's images to personal email accounts, personal cloud storage or personal devices;
- never share images through personal messaging or social-media accounts; and
- immediately report any accidental or inappropriate image capture or sharing.

Children's images and personal information must be stored securely and handled in accordance with the nursery's Data Protection/Privacy Policy and retention arrangements.

Children's Use of Technology

Technology used by children must have a clear purpose and support their learning and development.

Children will not access or use screens alone, or with other children, without adult supervision.

Practitioners will:

- closely supervise children when using electronic devices;
- ensure content is age appropriate;
- check websites, applications, videos and digital resources before children access them;
- check search results before displaying them to children;
- use appropriate safety settings and filtering;
- avoid unnecessary sedentary screen time;
- balance technology with active, physical, creative, social and outdoor experiences;
- model healthy and safe use of technology; and
- use technology as a tool rather than allowing it to replace meaningful adult interaction.

Staff should remain alert to advertising, pop-ups, links, autoplay functions and other content which may result in children accessing material that has not been intentionally selected.

Filtering, Monitoring and Internet Access

We will take reasonable steps to prevent children and staff from accessing inappropriate or harmful online content through our systems.

Appropriate filtering and security arrangements will be in place on our internet connections and devices.

Leaders will understand:

- what filtering is in place;
- which devices connect to the internet;
- how devices connect to the internet;
- who has administrative access;
- how passwords are managed; and
- how concerns regarding inappropriate content or internet use can be investigated.

Filtering does not replace appropriate adult supervision.

Staff must never deliberately bypass, disable or interfere with filtering, security or monitoring arrangements.

Personal Mobile Phones and Devices

Personal mobile phones, smart watches, tablets, cameras and other devices capable of taking photographs, recording or accessing the internet must be used in accordance with the preschool Mobile Phone and Camera Policy.

Personal devices must never be used during working hours and are kept securely away from the children at all times.

Where staff require access to a personal mobile phone during the working day, this must follow the preschools agreed procedures, for example during lunch break away from the children or off-site.

Staff Social Media and Professional Boundaries

Staff must maintain appropriate professional boundaries online as well as in person.

Staff must never:

- discuss confidential information about children, families, colleagues or the preschool on social media;
- post photographs or information which could identify a child without appropriate authority;
- use personal social-media accounts for routine communication with families;
- make comments online which could compromise children's confidentiality or safeguarding;
- post content which could reasonably bring their professional role or the preschool into disrepute; or
- use social media to discuss safeguarding concerns, complaints or confidential preschool matters.

Communication with parents/carers should take place through preschool-approved communication channels.

Staff are strongly advised not to accept friend/follow requests from current children or their family members through personal social-media accounts.

Where a pre-existing personal relationship exists, this should be declared to the manager/DSL so that appropriate professional boundaries can be considered and agreed.

Staff should remember that privacy settings cannot guarantee that information shared online will remain private

Messaging and Communication

Preschool business must be conducted through approved nursery systems wherever possible. This may include:

Brize Norton Village Preschool emails
Brize Norton Village Preschool Facebook page/ Closed Parent Group
Brize Norton Village Preschool telephone/mobile
Staff must not use personal messaging services or personal email addresses to share confidential information about children.

Where staff WhatsApp groups or similar communication platforms are authorised for operational communication, children's confidential or sensitive personal information must not be shared unless the platform and use have been specifically approved for that purpose.

Safeguarding concerns must always be recorded through the preschool's formal safeguarding procedures and must not rely upon messages within staff group chats.

Lost or Stolen Devices

Any nursery device that is lost, misplaced or stolen must be reported to the manager/DSL immediately.Staff must not wait to see whether the device is found before informing management.

The manager will establish:

1. Which device has been lost/stolen.
2. When and where it was last seen.
3. Who had access to it.
4. Whether it was password/passcode protected.
5. Whether remote tracking is available.
6. What personal information could be stored on or accessed through the device.
7. Whether photographs or information about children could be accessed.

Where possible, the nursery will immediately:

- remotely lock or wipe the device;
- change relevant passwords;
- revoke active sessions/account access;
- contact the police where theft is suspected;
- preserve relevant evidence;
- record the incident; and
- undertake a data-breach risk assessment.

Ofsted - A stolen device containing children's information is identified by Ofsted as an example of a significant event.

Where the incident meets the notification requirements, the registered provider will notify Ofsted as soon as reasonably possible and within 14 days of the significant event.

The setting will consider the circumstances of any lost device carefully to determine whether an Ofsted notification is required, particularly where children's information may have been accessible or children's welfare or safeguarding may have been affected.

What Happens if Inappropriate Content is Accessed?

If inappropriate, harmful or concerning content appears on a device being used with children, staff should:

STOP – prevent further access and calmly move children away from the content.

DO NOT SHARE – do not forward, screenshot, copy or unnecessarily reproduce concerning material.

REPORT – inform the DSL/manager immediately.

RECORD – make a factual record of what occurred, including the device involved, application/website, time and circumstances.

SAFEGUARD – where the content raises concerns about a child or individual, follow the nursery's Safeguarding/Child Protection Policy immediately.

Staff must not independently investigate safeguarding concerns or search for illegal content. Where appropriate, concerns may need to be referred to external safeguarding agencies, police, CEOP or the Internet Watch Foundation.

Online Safety Concerns

Online safeguarding concerns are treated in the same way as any other safeguarding concern.

Staff must report concerns immediately to the DSL where they become aware of:

- inappropriate or sexualised online content involving a child;
- online grooming or concerning communication;
- children being exposed to harmful or age-inappropriate material;
- concerns regarding photographs or videos of children;
- inappropriate staff use of technology;
- breaches of professional boundaries online;
- cyberbullying or online harassment;
- extremist or terrorist material;
- suspected illegal online content; or
- any other online activity which may place a child at risk.

The DSL will determine whether the concern requires referral or reporting to Children's Social Care, police, LADO, CEOP, the Internet Watch Foundation or another relevant agency.

Allegations or concerns regarding a member of staff must be managed in accordance with the Preschool's Safeguarding/Child Protection and Allegations Against Staff procedures.

Prevent Duty

We recognise that online environments can expose children and adults to extremist material.

Appropriate filtering will therefore be maintained to reduce the risk of children accessing terrorist or extremist content through preschool internet connections or devices.

Any concerns relating to radicalisation or extremism will be reported immediately to the DSL and managed in accordance with the nursery's safeguarding and Prevent Duty procedures.

Supporting Children to Understand Online Safety

Online safety will form part of children's wider safeguarding education in an age and developmentally appropriate way.

This may include supporting children to understand:

- that technology should be used with trusted adults;
- asking an adult for help if something appears that worries or confuses them;
- that some things belong to them and should not be shared;
- asking permission before taking photographs;
- respecting other people's photographs and information;
- that not everything seen on a screen is necessarily true;
- healthy boundaries around technology; and
- who they can talk to if something makes them feel uncomfortable.

This will be embedded naturally through conversations, stories, play and everyday experiences rather than relying solely upon specific online-safety activities.

Working With Parents and Carers

We recognise that children's experiences of technology extend beyond our preschool.

We will work collaboratively with parents and carers by:

- explaining how technology is used within the setting;
- sharing our expectations regarding photographs and digital information;
- obtaining appropriate permissions;
- sharing age-appropriate online-safety information;
- encouraging conversations about safe internet use at home;
- signposting families to reliable online-safety resources where appropriate; and
- supporting families where online safeguarding concerns arise.

Staff Training and Responsibilities

All staff will receive information about this policy during induction and will be expected to understand and follow it.

Online safety will form part of safeguarding updates and training. Staff must understand:

- their individual safeguarding responsibilities;
- acceptable use of preschool technology;
- professional boundaries online;
- procedures for photographs and recordings;
- how personal data should be protected;
- how to report an online-safety concern;
- what to do if a device is lost or stolen;
- the importance of appropriate filtering and supervision; and
- how to report concerns regarding another member of staff.

Any deliberate misuse of preschool technology or serious breach of this policy may result in disciplinary action and, where appropriate, referral to external safeguarding or regulatory agencies.

Monitoring and Review

Leaders will monitor implementation of this policy through:

- supervision and observation of practice;
- regular checks of nursery devices;
- checks of access permissions and staff accounts;
- review of filtering and internet-safety arrangements;
- monitoring compliance with photograph and data procedures;
- discussion of online safety during staff meetings/safeguarding updates; and
- review of any incidents, concerns, breaches or near misses.

This policy will be reviewed at least annually, and sooner where:

- legislation or statutory guidance changes;
- new technology or digital systems are introduced;
- a safeguarding or online-safety incident occurs;
- a data breach occurs;
- monitoring identifies weaknesses in practice; or
- learning from local or national safeguarding incidents indicates that changes are required.