Online Safety and IT-related policies

Key information about this (combined) policy:

Policy Reference	ECCC-033
Version Number	v1.0
Date Issued	16 September 2026
Date of Review	September 2026
Approved By	Co-Director; Operations

Including

Online Safety Policy
Cyber Security Policy
Acceptable Usage Agreement
Mobile Phone and Electronic Device Use Policy
Photography and Filming Children Policy

Online Safety Policy

Policy Purpose

ECCC is aware of the growth of the internet and technology and the advantages this can bring to everyday life. However, it is also aware of the dangers it can pose and we strive to support children, staff and families to use the internet safely.

We refer to 'Safeguarding children and protecting professionals in early years settings: online safety considerations' to support this policy.

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Izzy Ruddick (DSL), or one of the Deputy DSLs.**

Any breach of this policy will be dealt with in line with the Child Protection policy and staff Disciplinary Procedures.

Easton Community Children's Centre (ECCC) Policy
Status: Approved

Scope, Application, Access

- The policy applies to all staff, parents, children, volunteers, contractors.
- The policy applies at all times and locations of work or when children are in our care.
- Policy available to: All staff, Current Parents, Public

Areas of risk

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation with technology often providing the platform that facilitates harm.

At ECCC, children's access to technology is extremely limited, and is always facilitated by an adult (see Screentime Policy). Therefore, the primary risk factor for children regarding technology in the setting is exposure to harmful, illegal or inappropriate content. This may include:

- Violent images or videos
- Pornography
- Extremist, racist or radical views
- Misinformation or fake news
- Inappropriate language or content for children's developmental stage

Why Use the Internet?

The Internet is an essential resource to support teaching and learning, therefore it is important for children to learn to be safe online from an early age; our setting can play a part in this process. Digital skills are vital to accessing life-long learning and employment. Children may use the internet outside of the setting and need to learn how to keep safe online.

Policy

1. Key online safety measures and how they will be managed

Filters and content blockers
The setting's DSL, in conjunction with the Co-Director; Operations and Operations Manager, will ensure that the appropriate filters are applied to the electronic devices in the setting and to the electronic devices used by staff and children. They will also review/monitor the sites accessed on a regular basis. The following will be checked as part of an audit of all digital devices used

- Operating systems controls
- Back up of important information

- Device safety settings
- Ensuring we have appropriate antivirus software on all devices and update them regularly
- Ensuring all devices are password protected and have screen locks.
- Ensuring content blockers and filters are applied to our internet connection.
- Reviewing any apps downloaded onto devices that could be used with children, ensuring they are age and content appropriate
- Ensuring no social media or messaging apps are installed on Nursery devices that could be used with Children.

Safe storage

- All Nursery devices must be stored in the secure cupboard in the Office at the end of each day.
- Personal electronic devices with imaging and sharing capabilities (mobile phones, smart watches) must not be used in the classrooms/garden or any location children are present. (see Mobile phone and electronic device use policy)

Photos

- Staff will only use nursery devices to record and/or photograph children in the setting, and will do this in line with our Photography and Filming Children Policy.

Internet use

- Children will never access online content (Internet and Alexa) independently. Staff guide and facilitate any use of online content.
- Any online content used with children will be reviewed in advance to ensure its content is age appropriate and effective in facilitating curriculum delivery.
- Any unsuitable content witnessed by staff or children, even accidentally, must be reported to the DSL.
- If a staff member discovers that an unsuitable site has been accessed on any of the settings electronic devices, they must report this to the DSL immediately.

Emails

- Staff will report emails with inappropriate content to the DSL and internet watch foundation (IWF www.iwf.org.uk)

The DSL will:

- Oversee internet use, training staff and developing online safety strategies for children and parents.
- Follow any concerns relating to online safety through our Child Protection Policy

- Provide training for staff, at least annually, in online safety and understanding how to keep children safe online.
- Report emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)

2. Helping children keep safe online

Staff will communicate with children about how they can be safe online. In conversations with children about online safety, we will focus on:

- Modeling language of 'safety' when guiding online use (i.e. when using YouTube to show a video of something for educational purposes - *"I am not clicking on pictures I don't know, I am being safe"*)
- Informing children about how to 'speak up' if they see something that makes them sad/worried/scared/angry or unsafe.

We monitor children's screen time to ensure they remain safe online and have access to material that promotes their development. All staff must follow our **Screen Use Policy.**

3. Parents/carers and online safety

- Parents/carers are not allowed to bring children's personal devices to ECCC.
- Parents/carers' attention will be drawn to the ECCC's Online Safety Policy.
- While on the premises parents/carers will be asked to comply with the setting's mobile phones/digital devices and online safety rules.
- Parents/carers accessing their child's personal online learning journal accounts from home will use their personal emails and passwords.

4. Managing content and Information systems

- All IT equipment is audited and checked at the beginning of each academic year by the operations team and thereafter is checked regularly. The security of the setting's internet is protected by monitoring/filtering managed by Unity Technology Services. All laptops have virus protection installed and all devices are updated regularly.
- Website photographs that include children will be selected carefully in line with our Photography and Filming Children Policy. The emerging threat of misuse of AI tools to generate intimate images of children will be carefully considered.
- Children's full names will not be used anywhere online, particularly in association with photographs.
- Written permission from parents or carers for featuring their child on the website is requested for specific photographs. Parents/carers may change this consent at any time by contacting the setting.

5. Communication

All staff must be aware of the need to manage our digital reputation, including the appropriateness of information and content that is posted online, both professionally and personally.

We will ensure all electronic communications between staff and parents/carers is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses, Famly accounts, and telephone numbers. This is to protect staff, children and parents/carers. Staff are not to share their personal contact details with parents/carers.

Principally, day-to-day communication with families is via Famly, our nursery management software.

Email is another useful way to communicate with parents about current activities and events in the setting.

- The setting's main email login details are known to the Office Manager and Senior Management Team; they are not shared with other members of staff to ensure confidentiality.
- Staff using email to communicate with each other or with parents/carers will use an ECCC email address.
- All emails sent to parents/carers are via the setting's/professional email address/es and never from a private/personal email address. When sending emails' all email addresses are kept private. When sending out bulk emails to parents, the email addresses of other parents will never be displayed.
- The setting's email addresses must not be used for personal email.

6. Staff use of the setting's electronic devices

- Staff will not use the setting's electronic devices for personal use.
- The setting will ensure that all programs used and websites accessed are appropriate
- All setting files that contain personal data will be stored appropriately and securely, e.g. on a drive with restricted access, or locked away.
- Staff will not forward any of the setting's work, files, information etc stored on the setting's electronic devices to their personal electronic devices, unless this has been agreed and recorded by management as necessary. Any work taken home will be protected as if it were in the setting and open to scrutiny by management.
- Generally, all IT equipment should remain in the setting. This is to minimise the risk of computer viruses and for data protection purposes.
    - Senior team members may take a laptop home with permission from a Co-Director.
- Staff will not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
- All email communication will be appropriate and written in a professional manner.

- Illegal or inappropriate materials MUST NOT be uploaded, downloaded or accessed.
- Staff will ensure that setting's electronic devices are used appropriately to avoid disabling or damaging equipment.
- Famly accounts with access to children's information will only be accessed by staff from a setting device.

7. Social Networking/Media Sites

Social networking sites (e.g.: Facebook, Instagram, WhatsApp, LinkedIn) can be a useful advertising tool for settings and can often be an effective way of engaging with parents/carers. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites.

- Staff, volunteers, students or management must not put details of their work on any form of social networking site without approval from a Co-Director.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- No staff are permitted to 'friend' parents/carers currently accessing the setting. Staff will declare any pre-existing friendships with parents/carers to their line manager and commit to keeping strict work /life boundaries.
- Staff, volunteers, students or management must not engage in any on-line activity that may compromise their professional responsibilities.
- Staff, volunteers, students or management must be very cautious about the content they post online. Everyone in the setting must be mindful that once content is placed online, even if swiftly removed, can remain accessible to all long-term.
- Recognisable photographs, names of, or comments about children within the setting must never be placed on any social networking site. Photos not showing any children's faces may be used.
- All staff, volunteers, students and management must not correspond with the setting's children/families through social networking sites.
- Staff will not discuss individual children or their setting on any social networking site.
- Staff should be aware of possible professional implications/risks when entering any personal details on any gaming or social networking sites (e.g.: YouTube, Facebook, Instagram, twitter etc).
- Staff should be aware that potential employers may conduct online/social media searches when recruiting.
- Staff will not be permitted to use the setting's electronic devices to access social networking sites at any time, including designated breaks.
- All communications in the setting will be transparent and open to scrutiny.
- All staff must be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.

8. Handling Complaints

Any complaints about the appropriate use of the internet or other technologies will be handled through the setting's existing Concerns and Complaints Procedure. Any immediate concerns about child welfare, or children accessing inappropriate content must be reported to the DSL as set out above.

Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) will ensure:
    - All staff know how to report a problem and when to escalate a concern, including the process for external referral
    - All concerns are logged, assessed and actioned in accordance with the ECCC's safeguarding procedures
    - Parents/carers are supported to develop their knowledge of online safety issues concerning their children. Parents/carers are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern
    - Staff have access to information and guidance for supporting online safety, both personally and professionally
- Operations Manager: Responsible for overseeing implementation of secure internet connection, filtering, and device security.
- All Staff: Responsible for adhering to the policy procedures at all times.

Related Documents and Legislation

- Other policies
    - Data Protection Policy
    - Privacy statement
    - Screen Use Policy
- Help for early years providers : Screen use
- Baby and toddler screen time guidance - Best Start in Life
- Safeguarding children and protecting professionals in early years settings: online safety considerations**:**
    - Safeguarding children and protecting professionals in early years settings: online safety considerations for **managers** - GOV.UK (www.gov.uk)
    - Safeguarding children and protecting professionals in early years settings: online safety guidance for **practitioners** - GOV.UK (www.gov.uk)
- Data Protection - Information Commissioners Office, detailed information on all aspects of data protection: https://ico.org.uk/
- Internet Matters - Helping parents keep their children safe online: www.internetmatters.org
- Common Sense Media - reviews information and age ratings on all sorts of media: https://www.commonsensemedia.org/
- National Cyber Security Centre

    - Early Years practitioners: using cyber security to protect... - NCSC.GOV.UK
- Cyber security standards for schools and colleges
    - Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK
- UK Safer Internet Centre - Advice and Report Harmful Content Centre: https://www.saferinternet.org.uk/
    - POSH (Professionals Online Safety Hotline) Professionals Online Safety Helpline - UK Safer Internet Centre Monday to Friday 10:00am - 4:00pm
    - For help and support, please email helpline@saferinternet.org.uk
- Internet Watch Foundation - To report images of child sexual abuse - Eliminating Child Sexual Abuse Online - Internet Watch Foundation (iwf.org.uk)

Easton Community Children's Centre (ECCC) Policy
Status: Approved

Cyber Security Policy

This policy should be read in conjunction with the Data protection and confidentiality policy, Online safety policy (above) and the Acceptable use agreement (below).

At ECCC we recognise that the key to keeping our nursery cyber secure is through effective staff systems, practices, and training so that everyone is aware of the actions they should take to protect our systems from threat.

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity, e.g. scam emails. All staff are reminded to follow our procedures including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

Procedures

How to contact our IT Support provider

Call: 0330 024 8222 Or, Call Tim Brice: 07808175982
Email: Support@unity-tech.co.uk
The Operations Manager or Co-Director; Operations can provide further information if required.

Passwords

We will:

- Create strong and memorable passwords for important accounts, such as by combining three random words. We will avoid using predictable passwords, such as dates, family and pet names. Passwords will not be reused
- All staff must use a separate password for work and personal accounts
- For office-based staff, passwords will be stored using password managers with end-to-end encryption
- We use multi-factor authorisation (MFA) to log in where appropriate, e.g. banking websites.

Security

- We inform staff about how to recognise the techniques that phishers use in emails, as well as recognising spam and other harmful content
    - Staff are not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

- Staff must report suspicious messages or links to the Operations Manager and IT support as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious email reporting service at report@phishing.gov.uk.
- We carry out regular software updates and regularly check our back-ups
- Staff always lock devices in locker when not in use
- We use PINs on portable devices
- We do not install any software that has not been cleared for use by the Operations Manager, a Co-Director, or IT support onto our computers or systems
- Unknown USBs or external devices will not be used on our systems.

Reporting

- Staff are encouraged to ask for further guidance or support from IT support when something feels suspicious or unusual
- Staff are encouraged to flag concerns and must report attacks as soon as possible.

System access

- We use a separate 'guest' WiFi for visitors to limit access to the office network
- We regularly review system access
- Accounts are removed immediately when a staff member has left employment.
- We limit access for temporary workers
- Staff follow sign-in/out protocols
- No staff member has access to nursery devices outside working hours, except where use of a laptop from home has been agreed by a Co-Director specifically.

Actions in the event of a cyber attack

- The Co-Director; Operations will be informed immediately of any actual or suspected security breach
- We will contain the breach, isolate affected devices and disable compromised accounts
- We will avoid deleting anything that could serve as evidence
- We will keep a log of actions taken and notify the Information Commissioner's Office (ICO) if personal data is at risk https://ico.org.uk/for-organisations/report-a-breach/
- We will seek advice and guidance from the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk/
- We will communicate clearly with staff and stakeholders to explain what's happened, what we're doing and how it affects families and staff
- Following an actual or suspected attack, we will review our systems to identify what occurred, what was compromised and what changes are needed.

Acceptable Usage Agreement

This document must be completed by all staff.

In addition to the requirements of the:

- Online Safety Policy,
- Cyber Security Policy,
- Mobile Phone and Electronic Device Use policy, and
- Photography and Filming Children Policy,

ECCC staff must not:

- Access or attempt to access, store or distribute any material which is:
  - Violent or which glorifies violent behaviour
  - Criminal or which glorifies criminal behaviour
  - Racist or designed to incite racial hatred
  - Pornographic or with otherwise unsuitable sexual content
  - Crude, profane or with otherwise unsuitable language
  - Mocking of religious or moral beliefs
  - In breach of the law – including copyright and data protection
  - The property of others, without explicit permission

- Search for or use websites that might bypass ECCC's Internet filtering

- Interfere with or cause malicious damage to ECCC's IT resources

- Install any software that has not been cleared for use by the Operations Manager, a Co-Director, or our IT support provider onto our computers or IT systems.

- Use any removable storage media which has been used on hardware not owned by us (e.g. USB pen drive, CDROM etc.). No unknown USBs or external devices (not owned and purchased new by ECCC) will be used.

- Remove any device, media or data from the premises, without explicit permission from a Co-Director.

- Access personal e-mail accounts, social media platforms or use any IT resources (including phones) for personal reasons:
  - at any time on room based devices
  - during work time on any device
  - Any use of our electronic communication systems (including email, internet and telephones) for purposes other than the duties of your employment, during work time, is not permitted.
  - Emergency personal calls need to be authorised by the manager and, where possible, be made on your own personal mobile phone outside the nursery.

- Re-use passwords, or fail to keep passwords for our systems confidential. You must not share any personal passwords with any other person; in particular you must not allow any other staff member to know or use your personal password. (We recognise that passwords for shared accounts, e.g. the room google account login, will be shared amongst staff that need to access them).

- Fail to immediately report any breach of this policy (deliberate or accidental) to a Co-Director.
    - Each employee has a responsibility to report any misuse of the internet or email. By not reporting such knowledge, the employee will be considered to be collaborating in the misuse. Each employee can be assured of confidentiality when reporting misuse.

- Fail to immediately report the loss or damage of any device. Any damage beyond reasonable wear and tear/accidental will be the employee's responsibility and at their cost to amend.

Aside from the use of tablets in rooms with shared 'room' logins, in regards to the use of Famly, staff will:

- Ensure that log in details remain confidential to themselves and the manager only.
- Not save passwords for Famly on home or personal digital devices.
- Not allow anyone else to access Famly if editing the programme at home.
- Not share the information stored on Famly with anyone other senior managers and appropriate staff.
- Ensure that they are logged out of the programme when not in use.

Breach of this agreement and our related policies may lead to disciplinary action, up to and including summary dismissal.

Declaration:

I confirm that I have read and understood these requirements and agree to comply with them.

Signed……Date……..

Print Name…….

(Alternatively, accepting this policy on BrightHR confirms you have read and understood these requirements and agree to comply with them)

Mobile Phone and Electronic Device Use Policy

Note: *For the purpose of this policy, the category of 'mobile phone' also includes other technological personal devices, including smartwatches and any other personal device with camera, video and recording technology.*

At **ECCC** we promote the safety and welfare of all children in our care. We believe our staff should be completely attentive during their hours of working to ensure all children in the nursery receive good quality care and education.

To ensure the safety and well-being of children we do not allow staff to use personal mobile phones or other personal devices with imaging and sharing capabilities during working hours.

We use mobile phones supplied by the nursery only to provide a means of contact in certain circumstances, such as outings.

This policy should be used in conjunction with our Online Safety Policy and Acceptable Usage Agreement, to ensure children are kept safe when using the nursery devices online.

Staff must adhere to the following:

- Mobile phones, or other personal devices with imaging and sharing capabilities are not accessed during working hours
- Mobile phones, or other personal devices with imaging and sharing capabilities can only be used on a designated break and then this must be away from the children (i.e. in the staff room, lounge, or nest spaces).
- Mobile phones, or other personal devices with imaging and sharing capabilities must be stored safely in staff lockers at all times during working hours
- No personal device is allowed to be connected to the main nursery Wi-Fi at any time, only to the 'ECCC Guest' network
- The use of nursery devices, such as tablets, must only be used for nursery purposes
- The nursery devices will not have any social media or messaging apps on them, except those used by the Senior Management Team for nursery purposes only
- Any apps downloaded onto nursery devices must be done only by a member of the Senior Management Team. This will ensure only age and content appropriate apps are accessible to staff, or children using them

- Passwords and/or passcodes for nursery devices must not be shared or written down (with the exception of shared 'room' logins), and will be changed regularly
- During outings, staff must only use mobile phones belonging to the nursery
- Only nursery owned devices will be used to take photographs or film videos. These devices will only be used in the presence of other staff
- Nursery devices will not be taken home with staff and will remain secure at the setting when not in use
- Digital photographs and videos of children will be stored securely in a drive folder with restricted access in accordance with our Safeguarding children and child protection policy and data protection law. Hard copies of images will be stored in a locked container
- We will never store digital images of children on unencrypted portable equipment such as laptops, memory sticks and other digital devices
- Staff must delete images/videos from devices, or store them in agreed folders, once they have been used for their purpose. Managers will check image folders regularly.

Parent/carer use of mobile phones and smartwatches

Parents/carers must refrain from using their mobile telephones, or other personal devices with imaging and sharing capabilities, whilst in the nursery or when collecting or dropping off their children. We will ask any parents/carers using their phone/device inside the nursery premises to finish the call or take the call outside. We do this to ensure all children are safeguarded and the time for dropping off and picking up is a quality handover opportunity where we can share details about your child

Parents/carers are requested not to allow their child to wear or bring in devices with imaging and sharing capabilities. This ensures all children are safeguarded and also protects their property as it may get damaged or misplaced at the nursery.

Visitors' use of mobile phones or other personal devices with imaging and sharing capabilities

Visitors are not permitted to use their mobile phones or other personal devices with imaging and sharing capabilities, e.g. smart glasses, whilst at nursery and are asked to leave them in a safe secure place, such as the front office, for the duration of their visit. A 'phone free zone' poster (or similar) will be displayed on entrances.

Digital photographs and videos

See the Photography and Filming Children Policy below.

- Written permission from parents/carers will be obtained and documented before any images of children are recorded. This may mean that separate permissions are needed for:
    - Evidence of EYFS tracking or play quality in the setting.
    - Use of images on setting website or other publicity.
    - Images recorded during events/ parties/fundraising or outings.
- Parents will be made fully aware of how any images of their children may be used and they have the right to decide if they wish their children to be photographed or not. Parents must also be able to have a say in how these photos will be used.
- Using Famly online learning journal and providing parent updates
    - At ECCC we use tablets in the rooms to take photos of the children and record these directly on to their electronic learning journeys. We ensure that these devices are used for this purpose only and do not install applications such as social media or messaging sites onto these devices.
    - We remind staff of the Whistleblowing policy if they observe staff breaching these safeguarding procedures.
- Digital images will be stored in a folder on our drive, which is accessed by setting practitioners only.
    - Photos should be deleted from setting tablets/phones once transferred to the drive.
    - Any cameras and memory sticks storing images will be locked away.
- While using digital images, practitioners will be aware of the risks associated with the taking, using, sharing, publishing and distribution of images.
- Setting practitioners will only use the setting equipment. Personal equipment will NOT be used to record images of the children.
- Staff will be vigilant when taking digital/video images of the children to ensure that they are appropriately dressed.
- Staff will be aware of any child/ren who are at risk or under a supervision order, so their images are not used.
- After a displayed photograph is taken down, it will be either stored in the child's file, deleted, returned to the family or shredded.

Responsibilities

Practitioners/volunteers should:

- Report any concerns about any inappropriate or intrusive photographs found or any activity that raises concerns to their line manager and the DSL and a record will be made.
- Be aware that failure to comply with policies and procedures may result in disciplinary action being taken.
- Be aware that not following the settings guidance is potentially a safeguarding and child protection issue which may affect their suitability to work with children.

Photography and Filming Children Policy

At ECCC we wish to share and celebrate our children's achievements, including images of activities, experiences and opportunities they enjoy. Photographs and videos help us document children's learning, communicate with families and, where appropriate, promote our setting through our website, social media channels and other publications.

The safety and wellbeing of every child is our highest priority. This policy explains how we take, use, store and share images of children safely, lawfully and respectfully.

We have a responsibility to promote the welfare of all babies and children through taking, sharing and using images of children safely so that they do not inadvertently experience abuse through:

- Images being misused out of context or modified using AI, for example to create child abuse images
- A child being identified for the purpose of future grooming and abuse
- A vulnerable child being identified by an existing perpetrator of abuse
- A child or family being located or targeted, such as for identity theft or impersonation.

We recognise that:

- Sharing photographs and films of our activities can help us celebrate the successes and achievements of our children, provide a record of our activities and raise awareness of our organisation
- There are potential risks associated with sharing images of children online and the welfare of the children attending our setting is paramount
- Children and their parents have a right to decide whether their images are taken and how these may be used, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation
- Consent to take images of children is only meaningful when children and their parents understand how the images will be used and stored and are fully aware of the potential risks associated with the use and distribution of these images.

General procedures

We will seek to keep our children safe by:

- Asking parents to sign a permission form as part of their induction when joining ECCC, supplying written consent to use children's images internally, such as for learning journeys
    - Clearly explaining how images will be used, stored and shared, including informing parents that once an image has been published online, it may not be possible to remove it if consent is later withdrawn
    - We ensure that parents understand that where their child is also in another child's photograph, but not as the primary person, that may be used in another child's learning journey.
- Photographs and videos will not be taken in areas where intimate care routines are carried out.
- Following our reporting procedures if we become aware of the abuse or misuse of images of our children.

For content that is shared externally (beyond display inside the ECCC building or with parents via the Famly app):

- Not naming the children whose images are being used in our externally published material
- Never publishing personal information about individual children
- We do not publish any photographs of our children on our setting social media accounts.
- Reducing the risk of images being copied and used inappropriately by:
    - Only using images of children in appropriate clothing,
    - Avoiding full face and body shots of children; where close-ups are used, we aim to use images that capture children side on
    - Using images that capture an activity from a distance, or exclude the child's face by capturing images of their engagement in the activity, e.g. just their hands
    - Using images that positively reflect children's involvement in the activity, experience or event and avoid images that may be prone to misinterpretation or misuse
    - Where children/s faces are visible we will reduce the resolution of images to limit the potential for them to be repurposed
    - Regularly reviewing the photo and video content on our website and social media platforms to assess if they meet the guidelines; where necessary, over time replacing images of children with more generic visuals or illustrations.

Photography / filming for personal use by parents/carers:

- We do not allow parents/carers to use any personal devices with imaging and sharing capabilities, or to take any pictures or videos while in the nursery or at nursery events **during our regular opening hours**.
- For our occasional events outside of our opening hours (such as leavers events, winter fair, etc) we will share guidance about image sharing before the start of an event where parents/carers or spectators are taking photographs or filming at our events and the images are for personal use.
    - We will stipulate that photos taken during the event are not to be shared on social media
- If parents/carers share photographs or images of their own children from the event, remind parents/carers that no other child must be present (unless permission from other parents/carers is gained prior to sharing photographs and videos that include their child).
- Reminding parents/carers to check the privacy settings of their social media account to understand who else will be able to view any images they share
- Reminding parents to talk to the designated safeguarding lead (DSL) if they have any concerns about images being shared.

Photography / filming for setting use:

- Staff must only take images or videos using the setting's own devices, as per the Mobile phone and electronic device use policy
- If we hire a photographer for an event, we will seek to keep our children safe by:
    - Providing the photographer with a clear brief about appropriate content and behaviour
    - Ensuring the photographer has a written agreement with the setting covering copyright, permitted use, secure transfer and deletion of images once received by the setting
    - Ensuring the photographer has a relevant DBS check
    - Ensuring the photographer wears identification at all times on site
    - Informing children and their parents/carers that a photographer will be at the event and ensuring they give written consent to images which feature their child being taken and shared
    - If a parent does not consent to photographs/videos being taken, we will respect their wishes and make arrangements which will be agreed in advance with the photographer so they are aware not to take images of the child, ensuring that this is done in a way that does not single out the child or make them feel isolated. We will never exclude a child from an activity because we don't have consent to take their image
    - Ensuring the photographer does not have unsupervised access to children

- Reporting concerns regarding inappropriate or intrusive photography following our child protection procedures.

We will store photographs and videos of children securely, in accordance with our Child Protection Policy and data protection law.