PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

As a setting we recognise that we live in a technological world that has become an integral part of our daily lives and is advancing all the time. We view technology as an essential resource which can support teaching and learning but at the same time recognise there needs to be safeguarding measures in place to keep children safe. It is also our duty to fulfil legal duties in relation to personal data and other areas and therefore the information that we hold about the children and families will be handled in a manner compliant with the GDPR of 2018.

As a staff team we want to be clear with regards to our roles and responsibilities with regards to the use of cameras, mobile phones, computers, smart devices, and games consoles within our setting.

Digital and Video Images:

- We will get written permission from parents/carers before any images of children are taken, recorded, and used for publicity events.
- Children's full names will not be used on the settings website or literature.
- Digital images will be stored on the tablets or in a named file on the computer which is only accessible by the setting staff.
- All images will be stored in accordance with data protection laws e.g.: password protected files, cameras and memory sticks locked away.
- Members of staff will be aware of the risk associated with taking, using, sharing, publishing and distribution of images.
- Members of staff will not access the children's learning journeys from home, adequate time will be given within their working hours to keep learning journey's up to date.
- Members of staff will only use the settings ICT equipment to photograph or record images of the children: personal equipment must NOT be used unless approved by the Managers in extenuating circumstances.
- Members of staff will be vigilant when taking digital and video images of the children to ensure they are appropriately dressed.
- Group photographs and videos will be used in learning journeys to demonstrate and evidence their social skills.
- Individual parent and carer's wishes will be respected.
- After a photograph is taken down off a display it will be either stored in the child's file, returned to the family, or shredded.

- When booking a professional photographer in to take children's photos, we will ensure the photographer has an up-to-date DBS and will be supervised when with the children.

- No child will be forced to have their photo taken.

- Parent and carer's have the right to request their child be excluded from photographs and videos.

Mobile Phones:

- Members of staff are not permitted to have their mobile phones on their person or in the rooms where children are present.

- Mobile phones must be kept in a secure area away from where the children are accommodated.

- Members of staff may use their mobile phones during their designated breaks in an area away from the children.

- The settings main phone number can be given as a contact number in the case a member of staff needs to be contacted in work hours.

- Visitors and parents and carers are asked to not to use the mobile phones or smart devices whilst on the premises. If they need to use their mobile phone, they will be asked to do so away from the children.

Mobile phones on outings**:**

- Whilst on outings or trips, mobile phones may be used as a form of communicating with the setting or in cases of emergencies only. They should not be used for any other purposes e.g., a camera, for personal calls etc. unless approved by the Managers and this will only be approved under extenuating circumstances.

Acceptable use of wearable devices**:**

Smart watches and fitness watches are permitted to be worn by staff and visitors, including supply and agency staff, but must only be used as a watch and in line with the following guidelines:

- Notifications, connectivity, Apps, and Bluetooth must be disabled while on duty.

- The device must not have an in-built camera.

- Staff are not permitted to make or receive calls, texts, or emails via their wearable device while on duty.

- Staff are not permitted to access any form of social media via their wearable device while on duty.

- It is the responsibility of the individual to ensure this guidance is followed.
- Windmill Hill City Farm cannot take any responsibility for loss or damage to any personal device.

Any staff found to be misusing their wearable device may be subject to disciplinary action in line with our disciplinary procedure.

Any misuse of wearable devices when on duty should be reported to the Manager in line with the safeguarding and whistle blowing procedures.

Computers, Laptops and Tablets:

- Members of staff should not use the settings computer, laptop, or tablet for personal use.
- All setting files that contain personal data will be stored appropriately and securely, e.g.: password protected or locked away and accessible to only those who require this information.
- Members of staff will not forward any of the settings work, files, information etc. stored on the setting computer/laptop to their home PC, unless this has been agreed by management as necessary practice for the setting. i.e. home working.
- Any work taken home needs to be appropriately protected as if it were in the setting and open to scrutiny by management.
- Practitioners will not use any personal memory devices in the settings computer or laptop.
- Memory sticks provided by the setting should be used for work purposes only and should not be taken off the premises without permission from senior management.
- All ICT equipment will remain in the setting unless otherwise authorised by your manager. This is to minimise the risk of computer viruses and for data protection purposes.
- Practitioners must not share their unique and personal log in credentials (username and password) with other users.
- Email communication must be appropriate and written in a professional manner.
- E-mail attachments will only be opened if they are from a known and trusted source, to reduce the risk of the attachment containing viruses or other harmful programmes.
- Illegal or inappropriate materials will not be uploaded, downloaded, or accessed.
- Members of staff will ensure that the settings computer and laptop is used appropriately to avoid disabling or damaging equipment.
- Virus protection software is used and updated on a regular basis.

- Content filtering software is in place to minimise the risk of exposure to inappropriate materials.
- Children will always be supervised when they are accessing the internet.
- The setting will ensure that all programs used, and websites accessed are appropriate and children are not able to access or download material which is unsuitable.

<u>'Famly' E-Learning Diaries:</u>

- All users of 'Famly', whether it is a parent, carer, or member of staff, must sign the relevant agreement before use. The agreement will include the following:
    - Staff must not access 'Famly' on their own personal devices.
    - Staff may only access 'Famly' on Windmill Hill City Farm Computers and/or Tablets during working hours.
    - Parent and Carers are requested not to share, screenshot or upload photos/videos onto social media or for personal use.
    - All parties will ensure log in details are secure and not shared with unauthorised persons.
    - Where possible we will work with parent and carers wishes with regards to 'Famly' e.g., omitting a child from group photographs.
    - A copy of the 'Famly' security policy will be made available at request.

<u>Social Networking Sites:</u>

- Members of staff must not correspond with any child or family or share any information about a child or family on any form of social networking site (including photographs, names, or comments).
- Members of staff must not engage in any on-line activity that may compromise their professional responsibilities.
- Memerbs of staff should be aware of possible implications when entering any personal details on any gaming or social networking sites (e.g., YouTube, Face Book, Instagram, Twitter etc).
- Members of staff will be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.

<u>Computer Games and Gaming Consoles:</u>

- Members of staff will ensure that all games consoles and games used are suitable and appropriate for the ages of children in their care.
- Use of computer consoles should be supervised and monitored.

- All games used should be originals and not copies.
- Parents/carers will be made aware that IT resources including computer games which are age and developmentally appropriate will be available as part of the curriculum to the children.
- Children will be closely supervised to ensure that they are not accessing the internet via the console, or if they are permitted to do so that the websites accessed are appropriate and the setting has put in place appropriate safeguards.

How we support children's learning and development:

- How we use the Internet to enhance learning:
- Internet access is planned to enrich and extend children's learning activities. Staff will help guide the children with online activities that will support the learning outcomes for their stage of development.
- Children using ICT equipment.
- It is unfortunate that on occasions children may be confronted with inappropriate materials, despite all attempts at filtering the internet. A member of staff will oversee children and stay close so that they can intervene when necessary.
- We will ensure that children know how to ask for help if they come across material that makes them feel uncomfortable and is inappropriate.
- Members of staff will discuss e-safety when going through the settings 'Golden Rules' under the 'staying safe' rule.

Staff Responsibilities

- Report any concerns about any inappropriate or intrusive photographs or videos found.
- Report any activity that raises concerns.
- 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 a child protection issue which may affect their suitability to work with children.

All Adults Responsibilities

- Internet safety in the setting depends on staff, parents, carers, and visitors taking responsibility for the use of internet and other communication technologies such as mobile phones/smart devices.

- It is the setting's responsibility to use technical solutions and practices to limit internet access and to monitor their effectiveness.

To support families in keeping children under five safe online in the home environment we have devised an information sheet. Please see Appendix 1.

Further Information

South West Child Protection Procedures – provide detailed online information on all aspects of child protection : www.proceduresonline.com/swcpp/bristol/index.html

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/

Useful Contacts:

Board of Trustees Member responsible for Safeguarding & Child Protection: Susie Dunham

Designated Safeguarding & Child Protection Officer in the setting: Sophie Freyer

This policy works in line with our Safeguarding & Whistle Blowing Policy.

Appendix 1:

The digital world is here and whilst it can be exciting, educational, and interactive we want to support you in keeping your child safe when going online. Here are some questions, answers/advice to support you.

Question	Answer/advice
What internet compatible devices do you have in your home? (Phones, tablet, computers, games consoles & handheld consoles, Smart TV, Alexa, smart watches, camera, Fitbits, etc…) Which of these does your child have access to?	Parents/carers should ensure that all these devices have parental controls, filters, or passwords on them, so the risk of seeing or hearing unsuitable material is reduced (e.g., porn, violence, hatred). We recommend filters and parental controls are installed to reduce risk of accessing unsuitable material and passwords installed to control whether your child can download new apps or prevent them from purchasing downloads or in app purchases. Some parents set up a child's log in with selected websites, games, and apps. You can get detailed advice on how to do this from: https://www.internetmatters.org/parental-controls/
Where does your child use devices in the home?	It is recommended that all under 5's use devices in sight and hearing of their parent/carer. It is recommended that under 5's do not use headphones, so you can hear what is being said on these devices. It is recommended that children do not take devices into bedrooms or bathrooms as these are private areas and naked or nearly naked pictures are more at a risk of happening.
Where does your child use devices outside of the home?	It is recommended that all under 5's use devices in sight and hearing of their parent/carer. It is recommended that under 5's do not use headphones, so you can hear what is being said on these devices.
Do you go online with your child? What do you do together?	Exploring online can be a time to get to know and understand your child's internet use. Most games and devices have safety features that you can activate in settings. You can use this as a time to talk to your child about what's safe and what's not safe on the internet. It is good to start these conversations as young as possible with the expectation of having a continuing conversation throughout their childhood.

Have you set clear boundaries/rules for your child's online activities? What are they?	Being clear about what you expect is important. It is best to start conversations early about this. You may also want to use parental controls. Even if you have given a child a device as a present, it does not mean they should have it all the time. You might want to set boundaries about how long they spend online either daily or weekly (being clear on limits is important), where they can use devices and what to do if they see/hear something upsetting. Make sure children have device free zones, the bedroom and bathroom are recommended to reduce the risk of naked pictures being taken. Making sure children have device free time before bedtime is important to aid sleep. You could have a device box in your kitchen, so your child knows where the device is stored & when it can be used. For some young children a visual timetable may be useful.
Does your child know what to do if they see or hear something upsetting, worrying or if something unexpected happens? What do you tell them to do?	You could tell them to: - switch the screen off, - close the laptop, - turn over the tablet or phone - come and ask for help Have a conversation about what to do if they are worried. Let them know you are someone they can tell about anything that happens online and they are not in trouble.
Do you know where to go to get information about how to put filters on your broadband, parental controls on your devices and turn off online gaming? What have you already done?	You can find detailed advice on how to do this: https://www.internetmatters.org/parental-controls/ - Think about turning off location services on devices - Think about turning off in app purchases or restricting them with a strong password - Think about installing a child friendly browser - On some games you can turn off chat features/online gaming - https://www.net-aware.org.uk/ is a good site to check what apps are popular and what the positives /pitfalls of using them are. It also shows age rating. - https://www.commonsensemedia.org/ recommendations on apps, games and websites for children, with age recommendations
Does your child know to ask your permission before going on a new app, game or website?	Establish positive rules with young children – e.g. you must ask before… Under 5's struggle with negatives – e.g. : don't go on your brother's laptop

What do you tell them?	Explain why they must ask.
What do you tell your child about sharing information online?	Children have shared names, addresses, phone numbers, photographs. Young children often share too much, especially when asked direct questions. Tell your child if someone online is asking them questions that they need to come and tell you first to find out if they can, even if the person seems friendly. Talk to your child about why it's not ok
What do you share online? Do you leak information about your family accidently? What can you change to reduce risks to you and your children?	Adults may not be careful about their own privacy settings on social media (Facebook, Instagram, twitter) and so may leak information about their children's names, birthdays and images in school uniforms that other internet users can use to identify children or commit identity theft. Make sure that you are also Share Aware (NSPCC) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online/ http://www.bbc.co.uk/guides/z3b6y4j
What do you tell your child about other children/adults they may talk to online?	Children need to know that people (adults and children) can lie online about who they are. They need to know they should only be online "friends" with people they know and trust in the real world. Talk to them about what to do if a person/stranger wants to talk to them online, tell them to come and tell you first.
Do you know where to report online sexual abuse or grooming?	https://www.ceop.police.uk/safety-centre/should-i-make-a-report-to-ceop-yp/
Do you know where children can get support for online bullying?	https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/