

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY	
Reference: CF21	Effective date: 31.08.2012
Page no: 1 of 9	Approved: 31.08.2012
Last revision: September 2019	Revision date: September 2020



PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

As a setting we recognise that technology has advanced greatly and has become an integral part of our daily lives. As a setting we understand that technology is an essential resource to support teaching and learning but at the same time it is our aim to safeguard children in all possible ways and minimise the risk of harm. It is also our duty to fulfill legal duties in relation to personal data and other areas and therefore the information that we hold on our 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 any publicity events.
- Children's full names will not be used anywhere on the settings website or literature.
- Digital images will be stored on the tablets or in a separate file on the computer, which is accessed by the setting staffs only. These images will be stored in accordance with data protection laws e.g.: password protected files, cameras and memory sticks locked away.
- While using digital images, practitioners will be aware of the risk associated with taking, using, sharing, publishing and distribution of images.
- Setting practitioners will not access the children's learning profiles from home as practitioners will be given adequate time within their working hours to keep the learning profiles up to date.
- Setting practitioners will only use the settings ICT equipment: personal equipment must NOT be used to photograph or record images of the children unless approved by the Managers and this will only be approved for extenuating circumstances.
- Staff will be vigilant when taking digital/video images of the children to ensure that they are appropriately dressed.
- If a professional photographic company is coming in to take children's photos, the senior team will ensure that the photographer has an up to date DBS. No child will be forced to

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21

Effective date: 31.08.2012

Page no: 2 of 9

Approved: 31.08.2012

Last revision: September 2019

Revision date: September 2020



have their photo taken and parents can request if they do not wish for their child to have their photograph taken.

- Individual parent's wishes will be considered at all times.
- 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.

Please Note:

Where photos are taken of children interacting/playing with each other, these will be used in the appropriate children's learning diaries as these photos will provide evidence of their developing social skills. If this raises any concerns/issues please notify a staff member.

Mobile Phones and Smart Watches

- All individuals working directly with the children **will not** take their personal mobile phone or wear any smart devices in any of the rooms/areas that are used by the children.
- All mobile phones/smart watches will be kept in a secure area away from where the children are accommodated.
- Staff may use their mobile phones/smart watches during their designated breaks and in an area away from the children.
- The settings contact number will be given as an emergency number in case practitioners need to be contacted in work hours.
- Practitioners will be held responsible for the content and security of their smart devices, e.g. access to web pages. If this is deemed to be a safeguarding issue this will be dealt with in line with the settings safeguarding/child protection and disciplinary policy.
- Setting practitioners **will not** use any smart device cameras to photograph the children in their care.
- Visitors and parents will be asked to switch off their mobile phones/smart devices or not to use them 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 off site/on outings, 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. as a substitute for a camera, for personal calls etc. unless approved by the Managers and this will only be approved for extenuating circumstances.

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21

Effective date: 31.08.2012

Page no: 3 of 9

Approved: 31.08.2012

Last revision: September 2019

Revision date: September 2020



Computers, Laptops and Tablets

- Practitioners should not use the settings computer/laptop/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.
- Practitioners 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. 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/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 at all times 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 log in credentials (username and password) with other users. Log in credentials are unique and personal to each user. A user profile will be issued to any practitioner needing access to IT systems necessary for their work.
- All email communication will be appropriate and written in a professional manner.
- E-mail attachments will only be opened if they are from a source known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Illegal or inappropriate materials **will not** be uploaded, downloaded or accessed.
- Practitioners will ensure that the settings computer/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 in order 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 that children are not able to access or download material which is unsuitable.

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21

Effective date: 31.08.2012

Page no: 4 of 9

Approved: 31.08.2012

Last revision: September 2019

Revision date: September 2020



Tapestry E-Learning Diaries

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

Social Networking Sites

- Children's details (including photographs, names or comments) must not be entered onto any form of social networking site.
- Personnel must not engage in any on-line activity that may compromise their professional responsibilities.
- Adults in the setting will not correspond with setting children or families through social networking sites on a personal level.
- Practitioners should be aware of possible implications when entering any personal details on any gaming or social networking sites (e.g. You Tube, Face Book, Twitter etc).
- All staff will be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.

Computer Games/Games Consoles

- Practitioners 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 and children encouraged participating in a broad range of activities.
- All games used should be originals and not copies.

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21

Effective date: 31.08.2012

Page no: 5 of 9

Approved: 31.08.2012

Last revision: September 2019

Revision date: September 2020



- 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. As a result, staff will oversee children and stay close by to ensure they can see the electronic device's screen so that they can intervene when necessary. As a setting, we will ensure that children know how to ask for help if they come across material that makes them feel uncomfortable/is inappropriate. 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 found or any activity that raises concerns.
- Be made 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 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.

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21

Effective date: 31.08.2012

Page no: 6 of 9

Approved: 31.08.2012

Last revision: September 2019

Revision date: September 2020



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.swcpp.org.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.common sense media.org/>

Useful Contacts:

Committee Member responsible for Safeguarding & Child Protection: Sally Viner

Designated Safeguarding & Child Protection Officer in the setting: Vadna Chauhan

As an organisation it is our responsibility to ensure that people working with the children are trustworthy and responsible to do so. DBS checks are carried out on all individuals who have contact with the children our care. This policy works in line with our Safeguarding Policy.

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY	
Reference: CF21	Effective date: 31.08.2012
Page no: 7 of 9	Approved: 31.08.2012
Last revision: September 2019	Revision date: September 2020



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 & hand held 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.

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21	Effective date: 31.08.2012
Page no: 8 of 9	Approved: 31.08.2012
Last revision: September 2019	Revision date: September 2020



<p>Have you set clear boundaries/rules for your child's online activities? What are they?</p>	<p>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.</p> <p>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.</p>
<p>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?</p>	<p>You could tell them to:</p> <ul style="list-style-type: none"> - switch the screen off, - close the laptop, - turn over the tablet or phone - come and ask for help <p>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.</p>
<p>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?</p>	<p>You can find detailed advice on how to do this: https://www.internetmatters.org/parental-controls/</p> <ul style="list-style-type: none"> - 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.commonsemmedia.org/ recommendations on apps, games and websites for children, with age recommendations
<p>Does your child know to ask your permission before going on a new app, game or website?</p>	<p>Establish positive rules with young children – e.g. you must ask before...</p> <p>Under 5's struggle with negatives – e.g. : don't go on your brother's laptop</p> <p>Explain why they must ask.</p>

PHOTOGRAPHY, VIDEO, MOBILE PHONE AND E-SAFETY POLICY

Reference: CF21	Effective date: 31.08.2012
Page no: 9 of 9	Approved: 31.08.2012
Last revision: September 2019	Revision date: September 2020



What do you tell them?	
What do you tell your child about sharing information online?	<p>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</p>
What do you share online? Do you leak information about your family accidentally? What can you change to reduce risks to you and your children?	<p>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</p>
What do you tell your child about other children/adults they may talk to online?	<p>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.</p>
Do you know where to report online sexual abuse or grooming?	<p>https://www.ceop.police.uk/safety-centre/should-i-make-a-report-to-ceop-yp/</p>
Do you know where children can get support for online bullying?	<p>https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/</p>