ACCEPTABLE USE OF ICT & ONLINE SAFETY POLICY

Released January 2019

Rev: 1.01
Revised June 2021 (v1.03)

Policy statement

hdc aims to promote the acceptable use of Information and Communication Technology (ICT), including computers, tablets, the Internet, land line and mobile phones, other mobile devices (including smartwatches), cameras and image-making equipment. The purpose of this policy is to provide an environment in which children and young people, parents and staff are safeguarded from the misuse of such technology, including the inappropriate recording and use of images. The **Safeguarding Designated Officer (SDO)** manages the implementation of this policy; working closely with each setting's Designated Safeguarding Lead (DSL). Humpty Dumpty Childcare is registered with the Information Commissioners Office (ICO) registration number Z9139595.

Online Safety

Our nursery is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers and strives to support children, staff and families in using the internet safely.

Keeping Children Safe in Education states *"The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:*

- ✓ *content: being exposed to illegal, inappropriate or harmful material;*
- ✓ *contact: being subjected to harmful online interaction with other users; and*
- ✓ *conduct: personal online behaviour that increases the likelihood of, or causes, harm"*

Within the nursery we aim to keep children (and staff) safe online by:

- Ensuring we have appropriate antivirus and anti-spyware software on all devices and update them regularly
- Ensuring content blockers and filters are on all our devices, e.g. computers, laptops and any mobile devices
- Keeping passwords safe and secure. These are not to be shared with anyone other than the DSL, who will keep a list of these.
- Ensure management monitor all internet activities in the setting
- Locking away all nursery devices at the end of the day
- Ensuring no social media or messaging apps are installed on nursery devices
- Management reviewing all apps or games downloaded to tablets to ensure all are age appropriate for children and safeguard the children and staff .
- Any apps downloaded onto nursery devices must be done only by authorisation by DSL to ensure only age appropriate and safe apps are made accessible to staff/children using them.
- Using approved devices to record/photograph in the setting

- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Ensuring children are supervised when using internet devices
- Integrating online safety into nursery daily practice by discussing computer usage 'rules' deciding together what is safe and what is not safe to do online
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not, comparing people in real life situations to online 'friends'
- We abide by an acceptable use policy, ensuring staff only use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated. This includes when taking children out on outings.
- Children's screen time is monitored to ensure they remain safe online and have access to material that promotes their development. We will ensure that their screen time is within an acceptable level and is integrated within their programme of learning.
- Routine checks of tablets are undertaken to monitor search history and emails sent from these devices.

Staff Email

All staff are to use professional business practice when using email. As email is not a totally secure system of communication and can be intercepted by third parties, external email is not to be used in relation to confidential issues unless using an enhanced secure system e.g. egress.

Emails are not to be used to send abusive, offensive, sexist, racist, disability-biased, sexual orientation biased or defamatory material including jokes, pictures or comments which could be potentially offensive. Such use may constitute harassment and /or discrimination which would lead to disciplinary action up to and including dismissal.
If you receive unwanted messages of this nature, you should bring them to the attention of your manager.

Acceptable use:

The Internet
The internet is part of everyday life. Knowledge and experience of ICT are considered essential and developmentally appropriate access to computers and the internet contributes significantly to children and young people's enjoyment of learning and development. However, the use of computers and the internet carries an element of risk. Our aim is to outline safe and effective use of the internet to enable children, young people and adults to use ICT resources in a safe online environment.

- Staff are not to use the internet facilities to visit, bookmark, download material from or upload material to inappropriate, obscene, pornographic or otherwise offensive websites. Such use constitutes misconduct and will lead to disciplinary action up to and including dismissal in serious cases.
  Each employee has a responsibility to report any misuse of 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.
- Nursery tablets are to only be used for nursery purposes in line with your job description. They are not to be taken home with staff and will remain secure at the setting when not in use. If a device is needed to be taken home due to unforeseen circumstances then the person taking this device home must ensure it is securely stored and not accessed by another other

individual and returned to nursery as soon as practically possible. The device is to be signed out/in with the Nursery Manager.

- Access to sensitive and personal data is restricted to authorised individuals. Such data will be password protected.
- The internet will only be used for business and nursery purposes.
- If ICT users become aware that password security has been compromised, the concern should be reported to the Nursery Manager (DSL). If the DSL is not available report immediately to DDSL.
- Every reasonable precaution should be taken to ensure the safe use of the internet.
- Children and young people should be enabled to use online technologies as relevant to their age and development. Such use should always be monitored by a supervising adult.
- Computers and gaming devices should be sited in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be closely monitored.
- All ICT users are responsible for reporting any concerns encountered when using online technologies to the DSL
- The SDO will ensure that all users are aware of the procedures that must be followed in the event of a potentially unsafe or inappropriate online incident taking place.
    - If a child or young person accidentally accesses inappropriate material, it must be reported to an adult immediately.
    - Appropriate action should be taken to hide or minimise the window.
    - The computer should not be switched off, nor the page closed, in order to allow investigations to take place.
    - All such incidents must be reported to the SDO, who must ensure a report of the incident is made and that any further actions deemed necessary are taken. This could lead to suspension pending and investigation.
- All official online communications should occur where possible through secure, filtered email accounts.
- All email correspondence should be subject to scrutiny and monitoring.
- All ICT users are expected to write online communications in a polite, respectful and non-abusive manner.
- ICT users are advised not to open emails where they do not know the sender or where the format looks suspicious.
- When using digital communications, staff and volunteers should only make contact with children and young people for professional reasons and in accordance with the policies and procedures of the setting.
- Staff should not share personal information or personal contact details with a child or young person; nor should they request or respond to any personal information from the child/young person other than that which might be part of their professional role, or if the child is at immediate risk of harm. If usure whether to respond to an information requestion, speak to your DSO/DSL. Failure to adhere to this criteria could lead to disciplinary action being undertaken.
- If staff and volunteers have a personal social networking profile, they must ensure that details are not shared with children and young people in their care or their family members. They should make every effort to keep their personal and professional online lives separate. Do not include any information about your place of work or comments about your work environment, colleagues, families or children that t you work with.
- The adding of children and young people, parents and carers as 'friends' to social networking sites should be avoided.
- Staff should not post information online which could compromise their personal integrity or bring Humpty Dumpty Childcare into disrepute.

- Users are not to browse, download or send material that could be considered offensive to colleagues.
- Non-standard screen savers are not permitted.
- Do not download external security other than those agreed by hdc.

Mobile Phones and other devices that accept calls, messages and video calling
Mobile phone technology has become more sophisticated over recent years and many devices now enable access to content and services such as the internet, social networking sites and instant messaging. The content of this policy also relates to all other devices that have the capacity to accept calls, messages and/or video calling Our aim is to protect children and young people from harm by ensuring the appropriate management and use of mobile phones by all individuals who come into the setting. Personal mobile phones or other devices capable of accepting calls etc are not to be used during working hours when with the children. (Staff can access these during their designated lunchbreak but only when not in the vicinity of the children)

- All staff, managers and visitors must ensure that their mobile phones are turned off or on silent and locked/stored away from children in a designated location managed by the DSL; out of the reach of children during nursery hours.
- Users bringing personal devices into the setting must ensure there is no inappropriate or illegal content on the device.
- The use of nursery devices, such as tablets, must only be used for nursery purposes.
- Nursery mobile phones supplied by setting will be provided as a means of contact in certain circumstances such as outings.
- Mobile phones etc are to be stored in the designated locker during working hours.
- Staff are to not to use the internet facility of smartwatches whilst working with children. This function is to be turned off, or if not possible the watch is to be stored with the mobile phones.
- Mobile phones, smartwatches etc can only be used on a designated break, which must be away from children.
- If any staff member has an emergency which requires them to keep their mobile close at hand, they should consult with their line manager and get permission for this. In this situation, any phone calls taken or made should be done so in an area of the setting away from the children. Ideally the staff member should give the nursery telephone number as the contact.
- Should a staff member need to make an emergency personal call during working hours, they are to seek permission from their Manager.
- Staff should not give out personal mobile numbers to children or parents/carers. If staff wish to undertake 'babysitting' for parents they must adhere to the Occasional working policy. It is essential that all staff maintain a professional relationship with stakeholders.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Nursery Manager.
- Any non-compliance will be taken seriously, logged and investigated appropriately in line with hdc's policies and procedures.

Parents and visitors' use of mobile phones, smartwatches and social networking
Whilst we recognise that there may be emergency situations which necessitate the use of a mobile telephone, to ensure the safety and welfare of children in our care and share information about the child's day, parents and visitors are kindly asked to refrain from using their mobile telephones whilst in the nursery or when collecting or dropping off their children.
If you are found to be using your phone inside the nursery premises you will be asked to finish the call or to take it outside the premises.

We promote the safety and welfare of all staff and children at all times and therefore ask parents and visitors to follow this policy to ensure that information about children, images and information do not fall into the wrong hands.
If visitors bring a mobile phone or similar device into the setting, they will be asked to leave this in the Nursery office for the duration of their visit.

Cameras and Images
The use of cameras is considered an essential and integral part of everyday life. As such, children and young people and early years practitioners should be encouraged to use such technology in a positive and responsible way. It is recognised, however, that digital technology has increased the potential for cameras and images to be misused. We aim to ensure safe and appropriate use of cameras and images through agreed procedures, in line with legislative requirements and aims to respect the rights of all individuals. We ensure that photographs and recordings are only taken of children for whom we have parental/carer consent. We obtain this when a child is registered; however, parents can alter their consent at any time.
Cameras and videos may also be used to support staff development; the images will be used generally during individual review meetings to support discussions about that staff members practice.

- All staff, managers and visitors must ensure that their personal cameras and recording devices are locked away, out of the reach of children during nursery hours.
- Users bringing personal devices into the setting must ensure there is no inappropriate or illegal content on the device. These are to be stored in line with mobile phone storage. It is recommended that these are not brought into nurseries.
- Children should only be photographed or filmed on video for recording their learning and development (Learning Journey) or their participation in events organised by the setting**.** Parents are asked to sign a Consent Form for this to be authorised. Nursery tablets only are to be used for these purposes.
- Consent must be obtained from parents and carers if their child is photographed amongst a group of children and where the image is to be included in the learning journey of another child.
- Only hdc's designated cameras/tablets are to be used to take any photo within the setting or on outings.
- Images taken must be deemed suitable and appropriate and should not put a child or staff member in any compromising position that could cause embarrassment or distress.
- All staff are responsible for the location of the cameras and tablets, which should be stored in a secure place within the setting.
- Images taken and stored on the camera must be downloaded as soon as possible, with the room leader/manager's consent and images should only be downloaded on site.
- Images of children and young people will not be displayed on the hdc's external website without prior explicit consent from the parent or carer.
- The taking or making of images in sensitive areas of the setting, for example toileting/nappy changing areas is not permitted.
- A child or young person's full name or other identifying information should not appear in captions alongside photographs on displays, especially where such images are likely to be viewed by the general public.
- Where press are invited to planned events to take photographs of the children and young people who take part, parental consent should be sought before the event. If a parent or carer chooses not to give permission for their child to be photographed in such circumstances, this right must be observed at all times.
- Parents and carers are to seek written consent from the Nursery Manager if they wish to take photographs or make videos within the setting. They should be mindful of others when using

photographic equipment and should ensure minimum disruption to other parents and carers during any event or production. Parents and carers will only be permitted to take photographs or make videos for their own personal use. The use of any such images and recordings for any other purpose, without express permission, is not allowed.

- During special events e.g. children's parties, staff may produce group photographs/videos to distribute to parents on request. In this case we will gain individual written permission for each child before the event. This will ensure that photographs/videos taken will be in line with parent choice. We ask that these are not posted on social media without the permission of all the children included in the picture.
- All images will be stored and disposed of in line with the Data Protection Act 2018 and GDPR 2018 All images and photographs will be permanently disposed of when no longer of use. They will be returned to the parent or carer, deleted and wiped, or shredded as appropriate.
- It is the responsibility of all members of staff to be vigilant and report any concerns to their DSL/DSO.
- Any non-compliance will be taken seriously, logged and investigated appropriately in line with hdc's policies and procedures.

Online Learning Journals

At hdc, we use tablets in 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 private applications on these devices. Specific tablet applications will be installed to ensure appropriate functionality. Use of the tablets will be monitored to ensure that safeguarding requirements are not breeched.

ICT Misuse

Any allegation which is made in respect of the intentional or unintentional misuse of any form of ICT, *including computers, the Internet, mobile phones and other mobile devices, cameras, image-making equipment*, *and smart watches* will be addressed in a responsible and calm manner. Allegations will be dealt with promptly, sensitively and fairly in line with agreed procedures. The overall priority is to ensure the safety and well-being of children and young people at all times. If it is suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the hdc Safeguarding/Child protection Policy and Procedures will be implemented with immediately.

- The SDO is responsible for the management and implementation of all practices, protocols and procedures detailed in this policy.
- All staff are responsible for observing practice and behaviours which may indicate signs of potential misuse.
- All incidents will be dealt with on an individual basis. The context, intention and impact of each incident will determine the response and actions to be taken.
- All online safety incidents will be recorded and monitored, and any potential patterns in behaviours to be identified.
- Disciplinary action will be taken where:
    - The privilege of using our equipment is abused; or
    - Unauthorised time is spent on personal communications during working hours.
- The following procedures should be followed for ***all*** incidents:
    - All incidents should be reported to the SDO. A written incident record should be made and the situation monitored.
    - The context, intention and impact of the misuse will be considered. Where deemed necessary the incident may be escalated to a 'serious' level.
    - If the incident relates to the inadvertent access to an inappropriate website, it should be added to a banned or restricted list and filters should be applied, where relevant.

    - In respect of misuse by children and young people, parents and carers must be informed of the alleged incident and should be advised of any actions to be taken as a result.
- The following procedures should be followed for ***serious*** incidents:
    - All serious incidents must be dealt with promptly and reported to the SDO and the registered person.
    - The context, intention and impact of the misuse must be considered.
    - Appropriate actions should be agreed between the SDO and the registered person. All details should be recorded accurately and legibly. The reason why any decision is made should also be noted.
    - If at any stage a child or young person is or has been subject to abuse, the hdc Safeguarding/Child Protection Policy and Procedures will be implemented with immediate effect.
    - If the incident relates to an allegation made against an employee, manager, volunteer or student, and there is a suggestion that a child or young person has been subject to any form of abuse, the Safeguarding/Child Protection Policy and Procedures will be implemented with immediately..
    - The Local Authority Designated Officer (LADO) must be contacted in the first instance in respect of any allegation made against an adult. Subsequent action may include the need to contact the Police and Ofsted.
    - No actions should be taken which might compromise any investigations and no actions should be taken without the authorisation of the investigative body. The procedures laid down by the investigative body should be followed at all times.
- Internal disciplinary procedures will be undertaken as appropriate to the context, intention and impact of the misuse and in accordance with hdc's policies. In cases of serious misuse, internal disciplinary procedures will not be undertaken until investigations by the relevant agencies have been completed. Legal or human resource advice will be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.

If any staff observe others failing to adhere to these safeguarding process associated with online safety and safe use of the internet and devices, you are to follow the Whistleblowing procedures.

Document Control

Author	Connie Willcocks – Founder
Version Number	V1.02
Document Status	DRAFT
Approved by	Connie Willcocks, Founder / Managing Director Wendy Edmunds, Head of Childcare
Date Approved	
Effective Date	1 January 2019

Version Control

Version	Author	Date	Changes

1.01	Wendy Edmunds	9 December 2018	First draft for comment
1.02	Wendy Edmunds	7 January 2019	Final draft
1.03	Wendy Ellis-Smith	16 June 2021	Updated