SAFEGUARDING IN ICT POLICY

WRITTEN BY RACHAEL DUNPHY | DATE: 16/09/2023

This policy sets out the obligations of Rachael Dunphy when using digital multimedia. The policy primarily deals with the use of any film and electronic photographic equipment used in the setting such as:

- Mobile phones
- Tablets
- Wireless and broadband access
- Gaming station with inbuilt cameras
- Webcams
- Computers and laptops with inbuilt cameras
- Digital cameras
- Video broadcasting and music downloading
- Go Pro Devices
- Devices that store images

I understand the educational benefits of the advancement of digital technology and all it offers. At the setting, I have taken advice from relevant professionals and have regular review meetings on how and when we use such digital technology. The photographs and videos we take in the setting are generally used for advertising and celebrating success and achievements of staff and children, as well as to communicate what the children are doing while in my care to their parents.

This policy seeks to ensure that images and video footage taken within and by me, are taken with consent from both the child (with capacity) and the parent. I also ask for direct consent from children, where appropriate, if they would like to feature in a video or photographic footage. The media is held with the legal consent and legitimate interest and in accordance with GDPR.

Therefore, this policy will aim to:

• safeguard children and young people by promoting appropriate and acceptable use of information and communication technology (ICT)
• outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems.
• apply to all individuals who are to have access to and/or be users of work-related or personal ICT systems. This will include children and young people, parents and carers, students, visitors and family.
• outline safe and effective practice in the use of the internet

• provide advice on acceptable use and effective control measures to enable children, young people and adults to use ICT resources in a safer online environment
• ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is to be in line with legislative requirements and will aim to respect the rights of all individuals
• protect children and young people from harm by ensuring the appropriate management and use of mobile phones by all individuals who come into contact with the setting
• ensure children and young people are empowered with the skills to manage the changes in technology in a safe and appropriate way and to be alert to the potential risks of such use
• ensure any allegation (made in respect of the intentional or unintentional misuse of any online technologies) is to be addressed to Rachael Dunphy in a responsible and calm manner
• ensure that children suspected to be subject to abuse will be supported properly with the Safeguarding Policy and Procedures being implemented with immediate effect. These procedures are also to be followed should an allegation of abuse be made against any practitioner, volunteer or student. The Safeguarding Policy is to take precedence over all others, and referrals must be made to the appropriate agency as deemed necessary
• keep up to date with terminology used such as the 'Metaverse' and be aware of how to ensure children are kept safe.

Promoting Safe Use of Technology Within my Practice

My responsibilities and duties are:

- researching and downloading appropriate apps on my mobile device
- sitting with younger children when they are using the computer
- talking to children on an age-appropriate basis about the dangers posed by the internet
- explaining that anything shared online or by mobile phone could end up being seen by anyone
- understanding what each child does online and know which websites they visit
- not allowing children in my care to visit social networking sites
- effective reporting and whistle-blowing where appropriate
- using the CEOP, Hectors World browser button and Report Abuse buttons.

Children and young people will be encouraged to:

- be active, independent and responsible learners
- abide by this policy
- tell a familiar adult about any access of inappropriate content or material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent)

Password Security

Maintaining password security is to be an essential requirement. I will:

- keep passwords secure.
- have strong passwords, for example, an impersonal combination of numbers, symbols and lower/upper case letters
- ensure that computers and laptops to be set to 'timeout' the current user session should they become idle for an identified period.

Internet Access

The following control measures will be put in place which will manage internet access and minimise risk:

- secure broadband or wireless access
- a secure, filtered, managed internet service provider and/or learning platform
- secure email accounts
- a secure password system
- online activity is to be monitored to ensure access will be given to appropriate materials only
- computers and gaming consoles are to be sited in areas of high visibility which can be closely supervised and online use appropriately monitored.

Cameras and Images

- The use of cameras and images will be managed sensitively and respectfully.
- All images will be used in a manner respectful of the eight data protection principles.
- General signed consent to take photographs or record images of children will be requested from the parents/carers on enrolment of their child.
- The purpose for taking any images is to be clearly explained and agreed.
- Images will not be taken of any child or young person against their wishes.
- A child or young person's right not to be photographed is to be respected.
- Photographs are not to be taken of any child or young person should they suffer an injury, whether it is to be considered accidental or non-accidental.
- Images of children and young people must only be taken when they are in full and suitable dress.
- The taking or making of images in sensitive areas of the setting, for example, the bathroom, are not to be permitted.
- It should be ensured that a child or young person's name or any other identifying information does not appear in any caption or accompanying text alongside their photograph, for example, on displays.

- Parents must be made aware that they are not permitted to 'publicise' another child or young person without the express agreement of the parent or carer concerned.
- It must be ensured that still images (including those which are to be displayed in digital photo frames) and video clips are to depict children and young people in an appropriate way.
- Should any press or photos be used for journalistic reasons, full parental permission will be first sought.
- Children will be learning how to use technological equipment and may photograph each other. Appropriate use of the device will be taught and parents advised of any inappropriate actions undertaken by children.
- Images are to be stored and disposed of securely in line with the Data Protection Act 1998 and 2018.

Mobile Phones

All mobile phone use is to be open to scrutiny.

- Children and young people are not to be enabled to have access to their own personal mobile phones should they choose. Any phones brought into the setting will be left in the back bedroom in the care of Rich Clutton (if he is working from home) or locked in there (if RC is working at the office). I will not be held responsible for the damage or loss of any device brought into my setting.
- All service users, including parents, carers, visitors and contractors should be respectfully advised that their mobile phones are not to be used in the setting.
- Should it be considered necessary for mobile phone calls and/or texts to be taken or made, efforts should be made to avoid any unnecessary disturbance or disruption to children and young people.
- No personal technological devices (from the children's home) are permitted at the setting.

Driving

Phone calls or texts will not be answered whilst driving.

My Use of Social Media

To help continuously improve my childminding practice, from time to time I may use childcare-focused websites and social media, such as child-minding groups on Facebook. When using these sites, I will follow my confidentiality policy and at no time will I give out the names or personal information of children in my care.

Misuse Procedure

It is to be acknowledged that no system or procedure can be considered 100% safe, secure, and fool-proof. It should therefore be accepted that the potential for ICT to be misused, whether intentionally or unintentionally will remain. The aim of the ICT safeguarding policy will therefore be to minimise such opportunities and risk.

Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where known, off-site.

- All incidents are to be dealt with on an individual case by case basis.
- All online safety incidents are to be recorded and monitored, and any potential patterns in behaviours should be identified to enable such issues to be addressed proactively and for protection to be afforded. Alongside the name, written reports are to include the context, intention and impact of such misuse. Where deemed necessary, the incident is to be escalated to a 'serious' level
- If the incident should relate to the inadvertent access to an inappropriate website, it is to be added to the banned or restricted list and filters are to be applied, where relevant.

In the event of misuse by a member of staff:

Should it be alleged, that a practitioner is to have misused any ICT resource in an abusive, inappropriate, or illegal manner, a report is to be made. Procedures are to be followed as appropriate, in line with the Safeguarding Policy. Should allegations relate to abuse or unlawful activity, the Local Authority Designated Officer, Ofsted or the Police will be notified as applicable.

In the event of misuse by children and young people:

Should a child or young person be found to inappropriately misuse ICT the following sanctions will be applied:

• Step 1: the matter will be discussed with the parents and the child or young person may be temporarily suspended from a particular activity.
• Step 2: If there are to be further incidents of misuse, the child or young person will be suspended from using the internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail and the most appropriate course of action will be agreed.
• Step 3: Should a child or young person be considered at risk of significant harm, the Safeguarding Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care and Ofsted.

In the event that a child or young person should accidentally access inappropriate material, it must be reported immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

The 'Hectors World Safety Button', is to be available to children and young people where online access is to be enabled. At a push of a button, the child's view of the screen will be obscured. Adults will immediately be alerted and should take immediate and appropriate action. Should a child or young person be subject to potential abuse, sexual requests or other inappropriate contact, the CEOP Report Abuse button is to be used to make a report and further advice is to be sought.

The following incidents must always be reported to the Police, Children's Social Care, Local Authority Designated Officer and Ofsted:

- Discovery of indecent images of children and young people.
- Behaviour considered to be 'grooming'.
- Sending of obscene materials
- Cyber bullying

It should be understood, that by not reporting such incidents, an offence may be committed.

Serious Incidents

- It is to be ensured that no internal investigation or interviews are to be carried out in respect of any allegations unless it is to be explicitly requested otherwise by an investigating agency.
- It is to be fully recognised that should allegations of abuse be made, Children's Social Care, the Police and/or the Local Authority Designated Officer will be the investigative bodies. It must therefore be ensured that no action is to be taken which could compromise any such investigations.
- Where applicable, any hardware implicated in any potential investigations of misuse is to be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers, and portable media technology.
- On completion of both internal and external investigations, or sooner where it is to be deemed appropriate, an online safety review is to be undertaken and policies and procedures are to be amended and updated as necessary. Revised policies and procedures will be circulated as applicable.
- The seriousness of such allegations is to be fully recognised, and it must be ensured that all such incidents are to be reported to the police immediately. No attempt is to be made to download, print or send any materials found. Further offences could be committed by doing so. Should potentially illegal material be discovered, as far as is reasonably practical, the equipment or materials found will not be touched. Computers or other devices will not be switched off unless authorised to do so by the police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary, the monitor should be turned off (but the computer remain on).

Media Attention

It must be recognised that should a serious incident occur, it will most likely attract intense media interest and speculation. On such occasions, every possible attempt is to be made to ensure that children and young people, parents and carers are protected from such influences.

An agreed media strategy will be implemented, and statements must only be released by authorised personnel in accordance with information sharing procedures. In all instances, the prime concern will be the safeguarding and welfare of the children, young people ,and their families. Advice will be taken from Services for Children and Young People where appropriate before any media engagement is to be undertaken.

My Local Authority Safeguarding contact details and procedures are:

My LADO contact details are: 01924 302155 / lado.referrals@wakefield.gcsx.gov.uk

My Agency Contact Numbers are – 07908882120 / 07411026299

Further information:

https://www.gov.uk/data-protection

https://www.gov.uk/government/publications/data-protection-act-2018-overview

https://ico.org.uk/for-organisations/guide-to-data-protection/

Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://www.ceop.police.uk/safety-centre/

http://hectorsworld.netsafe.org.nz/teachers/hectors-world-safety-button/

If you have any questions about my policy/procedures or would like to make any comments, please ask.

SIGNED DATED