06.3 Online Safety, Cyber Security

Cyber security is a growing safeguarding concern and we recognise the need to have procedures to ensure networks, data and systems are protected against cyber threats and help keep staff and pupils safe, particularly when using remote learning and teaching platforms. We will:

- ensure that we have information and processes to raise awareness of online safety and cyber security.
- use the recommended national and local guidelines on staff and pupils who may need to work remotely. Online concerns will cover a range of safety issues including:
- Using social media platforms.
- fraud and scams
- copycat websites, phishing e-mails
- identity theft
- cyberbullying/trolling, cyberstalking,
- online grooming, online radicalisation,
- offensive/illegal content including race hate
- child sexual exploitation online
- Youth produced sexual imagery (sexting, nudes, semi-nudes)

Staff and children will be made aware of online safety issues and concerns, through training and the curriculum. The early years setting will ensure that when children access technology at the setting it is used safely, and the setting will ensure that online safeguarding practice is in line with statutory requirements and best practice.

https://www.gov.uk/government/publications/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

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

All staff must ensure that they understand the setting's policy relating to online safety which will be part of induction and will be refreshed at team meetings and training. The updated safeguarding policy, which includes the settings online safety procedures, is shared with parents on the website or parents are given an updated copy.

Managing access to online technology and acceptable use:

The setting will ensure that access to the internet has appropriate parental controls actively in place and filters which are revised regularly and kept up to date in order to restrict access to unsuitable information including extremist materials or inappropriate images However, we are aware that no filters can be 100% secure and access to apps, computer games, videos, films, approved internet sites etc. will be age appropriate and staff will supervise their use.

The setting's manager will keep an up to date log of the number and type of technology which have access to the internet at the setting and how they are connected (i.e. 4G/5G or Wi-Fi etc.) and ensure that access is secure (i.e. passwords in place that are not accessible or easy to guess and screens are locked). Devices must be kept securely and in line with GDPR. The physical equipment/furniture should be considered when using devices (risk assessed and appropriate for children and/or adults).

Staff use whilst at work:

The use of this equipment by staff is restricted in-order to avoid distraction and disruption to the care of children and to minimise the opportunities for any individual (or group) to put children into potential risk of harm. There is a clear expectation that the use of personal mobile phones/devices by staff is limited only to allocated lunch and/or breaks and not in the setting with children present unless there is an emergency and agreed by a manager of how this will be managed in-order to keep children safe.

Online Bullying and Wellbeing:

Immediate action will be taken if there is any concern about online bullying or the wellbeing a child in our care. If staff are targeted on-line (i.e. cyber bullying) they should inform their manager who will take appropriate action.

Online safety concerns:

Internet safety rules will be shared with parents and displayed, and children will be taught, age appropriately, about the risks online. Staff will model good practice at all times. There will also be an incident log to report any breaches of the filters in place and access to inappropriate material (accidental or non-accidental) will be reported to the Designated Safeguarding Lead who will then record the incident and escalate the concern as appropriate.

This could include:
● Reporting safeguarding concerns about a child to Derbyshire's Starting Point
● Reporting illegal images such as child sexual abuse to the internet watch foundation Homepage | Internet Watch Foundation (iwf.org.uk)
● Reporting online abuse etc. the child exploitation and online protection centre (CEOP) www.ceop.police.uk/ceop-reporting/)

Further advice or guidance can be sought from: The UK Safer Internet Centre Helpline for Professionals: www.saferinternet.org.uk/our-helplines
UKCIS (Education for a Connected World):
https://www.gov.uk/government/publications/education-for-a-connected-world

Cyber security is a growing safeguarding concern and we recognise the need to have procedures to ensure networks, data and systems are protected against cyber threats and help keep staff and children safe, particularly when using remote learning platforms. We will use the recommended national and local guidelines on staff and children who may need to take part in home learning.

Early Years settings/Childminders should refer to NSPCC guidance, when engaging in remote learning. The guidance is unchanged since its previous update (April 20th , 2021).

https://learning.nspcc.org.uk/news/covid/undertaking-remote-teaching-safely#article-t op

Mobile Phones and Cameras

Photographs - will only be taken of children with parental permission using the setting's camera/tablet, and only those which will help the staff to support a child's learning and development or share events. Photographic files will be stored safely and not be kept once the child leaves the setting's care unless prior agreement is agreed with the parent. Personal mobile phones/devises must never be used in the setting by staff to take photos or record/share images of children, in any circumstances. Other adults are not allowed to take photographs or videos of children in the setting (unless permission has been gained by the setting from all parents of all children involved for a celebration event etc).

Storing Personal Data – The setting has registered with the Information Commissioner's Office (ICO) as it stores personal data. The storage of personal and digital information will 4/10/2021 13 Controlled upon completion Model CP and Safeguarding Policy for Group care Ofsted Registered settings and Ofsted Registered childminders working with assistants V1 2021/22 also meet the requirements of the GDPR (2018) and will be secured at all times through password protections for access and regular virus check updates and filters.

Social Media - Staff must not accept or request to be friends on social network sites with parents or children that attend the setting or make any contact by their personal phone/devices (If there is a pre-existing relationship then this should be discussed with the DSL and/or the manager who will consider how this will be managed and provide clear guidance and boundaries and record action taken).

Any misuse or incidents must be reported to a manager and the DSL immediately, who will take appropriate action and take advice from the LADO (and the police) and follow the setting's procedures. If the circumstances result in dismissal (or resignation prior to actions being taken) the details will be reported to the Disqualification and Barring Service (DBS).