E-SAFETY POLICY AND PROCEDURES

This Policy document relates to the operation of:
GBNFC Group

Grendon & Billesley Nursery at Grendon Rd, B14 4RB
GBNFC Children's Centre – based at the Chinnbrook Centre
GBNFC Group at the Chinnbrook Centre B13 0ET
Hollywood Pre-school Daycare - based at Hollywood J & I School B14 4TG

Date Agreed by the Management Board: **March 2019**

Review: **March 2020**

Signature:

E-Safety Policy

The internet is an accessible tool to children in early year's settings- game playing, mobile learning apps etc

All early years settings have a duty to ensure that children are protected from potential harm both within and beyond the learning environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

Aims

- To offer valuable guidance and resources to settings and practitioners to ensure that they can provide a safe and secure online environment for all children in their care.
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for dealing with misuse of any technologies both within and beyond the early years setting.

This policy applies to all staff, children, parents/carers, boards, committees, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above mentioned groups, such as mobile phones or iPads/tablets which are brought into an early years setting. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop or mobile phone.

Staff Responsibilities

Practitioners (including volunteers/students)

All staff have a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

Please see mobile phone policy

The ICT Technician is responsible for ensuring that:

- the setting's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- anti-virus software is installed and maintained on all setting machines and portable devices.
- The setting's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the E Safety Lead and the Designated Person for Safeguarding (Kerry Huntley/ Taryn Moss).
- Any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the e Safety Incident Log (policy central).
- They keeps up to date with e safety technical information in order to maintain the security of the network and safeguard children.
- The use of the setting's ICT is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead/ Designated Person for Safeguarding.

Broadband and Age Appropriate Filtering

Broadband provision is essential to the running of an early years setting, not only allowing for communication with parents and carers but also providing access to a wealth of resources and support. The settings use internet enabled devices, and educational games to enhance the learning experience of children or as online tools. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children.

- Filtering levels are managed and monitored on site via an administration tool provided by Link2ICT which is managed also in house by the management on

policy central, which allows an authorised staff member to instantly allow or block access to sites and manage user internet access.

- Age appropriate content filtering is in place across the setting, ensuring that staff and children receive different levels of filtered internet access in line with user requirements

Email Use

Staff

- The setting provides some staff with access to a professional email account to use for all work related business, including communication with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Staff must not engage in any personal communications (i.e. via hotmail or yahoo accounts etc) with parents who they have a professional responsibility for. On induction, practitioners are given a social media form which they list all friends or relatives that are part of the GBNFC Group. Once you are an employee, then staff are asked to disclose to a member of management, any friends or relatives who join the settings, and this question is asked at every supervision session.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites (e.g. Facebook) can be used to advertise and engage with young or hard-to-reach parents on the Children's Centre side of the organisation. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites.

- Identifiable images of children should not be used on social networking sites.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.

- Ensure that privacy settings are set to maximum and checked regularly.

- For safeguarding purposes, photographs or videos of looked after children must not be shared on social networking sites.

Photographs and Video

Digital photographs and videos are an important part of the learning experience in early years settings and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

- Written consent must be obtained from parents or carers before photographs or videos of young people will be taken or used within the setting, including displays, development books, setting website and other marketing materials.
- Staff will ensure that children are at ease and comfortable with images and videos being taken.
- Staff must not use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children.
- Setting-issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, will not leave the premises unless encrypted. In the case of an outing, all photographs are transferred/deleted from the setting's camera device before leaving the setting.

Laptops

Staff Use:

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the Manager.
- Personal use of setting laptops or computing facilities, whilst on site, is left to the discretion of the Manager and may be permissible if kept to a minimum plus used outside of session times.
- Where staff have been issued with a device (e.g. setting laptop) for work purposes, personal use whilst off site is not permitted unless authorised by

the manager. The settings laptop/devices should be used by the authorised person only.

- Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will ensure that setting laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- Setting-issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted. Staff use of iPads for Tapestry learning journals are to be used on site and are to signed in and out of the main office by management. (see Tapestry policy)
- Ipads are monitored regularly by management, daily and weekly checked by a member of the management team checking that the iPad's are not being misused.

Children's Use:

- Computers use must be supervised by an adult at all times and any games used must be from a pre-approved selection checked and agreed by the senior.
- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.

Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.

- Before purchasing or accessing any apps for staff or children's use, Managers will have a clear understanding of where and how children's data will be stored, including who has access to it and any safeguarding implications.

Data Storage and Security

- Sensitive data, photographs and videos of children are not stored on setting devices which leave the premises (e.g. laptops, mobile phones, USB Memory Sticks etc) unless encryption software is in place.