Coniston Early Years Centre Policy Document

Safeguarding and Welfare Requirement: Child Protection
Providers must have and implement a policy, and procedures to safeguard children.

High Quality Care for All Children
A Firm Foundation for Education

1.6 ICT and Internet Use (Acceptable Use of Technologies

Introduction.

The internet should be considered part of everyday life with children and young people seen to be at the forefront of this on-line generation. Knowledge and experience of information and communication technology (ICT) should be considered an essential life skill. Developmentally appropriate access to computers and the internet in the early years will significantly contribute to children and young people's enjoyment of learning and development. This policy forms part of our Data Protection policies and procedures to ensure compliance with the GDPR (General Data Protection Regulations) and the Data Protection Act 2018.
Children and young people will learn most effectively where they are given managed access to computers and control of their own learning experiences, however such use carries an element of risk. Early Years practitioners and managers, in partnership with parents and carers, should consider it their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.
This statement applies to the use of technologies on the registered premises of this setting and in any locations visited in connection with running the pre-school. It applies to technologies owned by the setting and those owned by others. The purpose of having a statement on acceptable use in the setting is to try to ensure that;

- Children in our care are kept as safe as possible
- All adults and children at this setting will be responsible users who are pro-active about their own safety; and
- This settings ICT technologies and users are protected from accidental or deliberate misuse which could put the setting and its users at risk.

Policy Statement

This policy will outline safe and effective practice in the use of the internet. It will 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.

The policy applies to all individuals who are to have access to or be users of work related

ICT systems. This will include children and young people, parents and carers, early year's managers and practitioners, volunteers, students, committee members, visitors and contractors. This list is not to be considered exhaustive.

This policy will apply to internet access through any medium, for example computers, mobile phones, tablets and gaming machines. Before the use of any new technologies they will be examined to determine potential learning and development opportunities. Their use will be risk assessed before considering whether they are appropriate for use by children and young people.

Responsibilities

The Designated Person for Safeguarding (DPS) is to be responsible for online safety and will manage the implementation of this policy. In our setting the DPS is Sarah Trussell

The Designated Person for Safeguarding will ensure:

- Day to day responsibility for online safety issues and will have a leading role in implementing, monitoring and reviewing this Policy.
- All ICT users are made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.
- Recording, reporting, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. This must include the creation of an incident log to be used to inform future online safety practice.
- All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings take place between members of the senior management team to discuss current issues and review incident reports.
- Effective training and online safety advice is delivered and available to all early years managers and practitioners, including advisory support to children, young people, parents and carers as necessary.
- Liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Procedures

Every effort will be made to ensure that this settings ICT technologies are used in a responsible way, so that there is no risk to the safety or security of the children or adults or to the safety, reputation or sustainability of the setting itself. This applies to technologies owned by the setting and to that owned by others.

Coniston Early Years Centre takes steps to ensure there are effective procedures in place to protect our children from the dangers associated with prolonged use of ICT and inappropriate internet content.

These procedures relate to the use of all ICT equipment used or purchased for use by Coniston Early Years Centre. We are committed to ensuring the safety, both physical and psychological of all children, staff, committee, students, parents and visitors to the setting and therefore require all of the above to adhere to our policies and procedures.

General ICT Safety

- All ICT equipment purchased by the setting will be stored securely in the designated office area, all computers are password protected to prevent tampering or access by unknown persons.
- In respect of computers they will have antivirus and suitable internet safety software installed from the outset.
- No member of staff, student, parent helper, committee member or visitor to the setting will be permitted to connect any external device to the computer that could allow the transfer of inappropriate content from such a device to the computer.
- Staff have individual files on the computers where they maintain records for their current key group and where photos are sometimes stored for use in the child's learning journal. Any documents such as summary sheets, or other similar documentation for the children is maintained on these computers and moved to the settings hard drive as and when appropriate.
- Staff will be encouraged to access training that the local government or other organisations may offer in respect of using ICT equipment and maintaining children's safety whilst using such equipment.
- We will work in partnership with the local authority in respect of guidance they issue in respect of ICT use and safety.
- Children will only be allowed to use the computer for a maximum of 15 minutes at any one time in order to avoid causing eye strain or any other known risk associated with the prolonged use of a screen.
- When children are using the computer to access the internet a member of staff will remain with them for the whole period in order to prevent inadvertent access to inappropriate content or material.
- All ICT equipment will be PAT tested annually in line with all other electrical equipment owned by the setting.
- Under no circumstances should any person upload/download any internet or other content to the computers to which children have access as this would seriously compromise the internet security measures in place, any person who acts in this way will receive a written warning.
- All staff are required to clean any ICT equipment used with the appropriate wipes that are located in both desk drawers. This should be done after each use to prevent the spread of COVID19 and other infectious illness.

Managing online access

Password security

- Maintaining password security is an essential requirement for early years managers and practitioners particularly where they are to have access to sensitive information.
- Early years managers and practitioners are responsible for keeping their passwords secure and must ensure they are updated regularly or when a breach of security is suspected, passwords will always be changed when a staff member leaves the setting.
- Sharing passwords is not considered to be secure practice. Where children and young people are to be enabled to create their own password a copy of such will be kept on file for reference.
- All computers and laptops should be set to 'timeout' the current user session should they become idle for an identified period.
- All ICT users must 'log out' of their accounts should they need to leave a computer unattended.
- If ICT users become aware that password security has been compromised or shared, either intentionally or unintentionally, the concern must be reported to the Designated Person for Safeguarding.
- The internet access for all users will be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution will be taken to ensure the safe use of the internet. However, it must be recognised that it is impossible to safeguard against every eventuality.
- The following control measures will be implemented which will manage internet access and minimise risk:
    - Secure broadband or wireless access ○ Secure email accounts. ○ Regularly monitored and updated anti-virus protection.
    - A secure password system ○ An agreed list of assigned authorised users with controlled access ○ Effective audit, monitoring and review procedures.

Keeping Safe

Adults (And where appropriate children);

- Will only use their own user names and passwords which will be carefully chosen so that they cannot be easily guessed and will not use any other person's username and password.
- Will ensure that all data (including business documents and files) are regularly backed up.

- Will not engage in any online activity that may compromise their professional responsibilities or compromise the reputation of the setting or the safety and wellbeing of staff or children.
- Will ensure that the personal data for any child or family is kept private and confidential, except when we are required by law or by the settings policy to disclose it to an appropriate authority.
- Will only transport, hold, disclose or share personal information about themselves or others, in ways agreed by this setting and will not send personal information by email as this is not secure, unless in circumstances where secure email addresses have been obtained such as those provided by the Access and Response Team for example.
- Will not send personal data electronically if security cannot be guaranteed.
- Will ensure that there are suitable filtering and security systems in place and that they are not bypassed.
- Will ensure that all photographs of children cared for by the setting which are taken on cameras owned by the setting are stored and used responsibly.

Promoting Safe Use by Children

Adults (and where appropriate children)

- Will model safe use of the internet and help children to learn to use technologies safely.
- Will take all reasonable steps to ensure that all use of the internet is supervised and deal with any issues that arise.
- Will supervise children's access to material on the internet to ensure children remain safe in view of the possibility of radicalisation in line with the Prevent Duty (June 2015)
- Will take immediate action in line with our settings policy if a child reports any concerns or if an issue arises that might compromise the safety of any users, or the security of the setting.

Communication and Sharing

Adults (and where appropriate children)

- Will communicate online in a professional manner and tone (this includes communication by text message) and will not use aggressive/inappropriate language nor compromise either the providers position or the reputation of the setting
- Will only communicate with children and parents/carers using official systems owned by the setting.
- Will be aware that any communication from a student or adult on these premises could be forwarded to the provider.
- Will only use chat and social networking sites that are approved by the provider and for activity which has been agreed by the provider. We accept that in today's

society parents often contact staff via this route and that this is almost unavoidable. Staff therefore must agree that they will only accept such communications where they are happy to do so. Staff must also agree to inform senior management of any such communication.

- Will not use a personal email address on the settings ICT systems unless given permission.
- Will not access, copy, remove or otherwise alter any other users files without their permission
- Will ensure that permission is obtained to use the original work of others and will credit them if it is used. We will not download or distribute copies of material (including music and videos) which is protected by copyright.
- Will only take images of children and staff where it relates to agreed learning and management activities and will ensure that parents/staff permission is obtained before the images are taken.
- Will ensure that, where these images are published (eg on the settings website or in a newsletter) it will not be possible to identify the children who are featured by name or to discover any other personal information about them unless specific prior permission has been sought and agreed by those involved.
- Will ensure that parental/staff permission will be obtained if images are to be published online or in the media.
- Will not use personal equipment (including cameras and mobile phones) to record images unless specific permission has been given.
- Will not keep images of children stored on personal equipment unless permission has been given. If this is the case we will ensure that these images cannot be accessed or copied by anyone else or used for any purpose unless given permission.

Research and Recreation.

Adults (and where appropriate children)

- Will ensure that technology equipment is not used to upload, download or access any materials which are illegal (eg child abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or are inappropriate or may cause harm or distress to others.
- Will not (unless permitted) make large downloads or uploads that might take up internet capacity.
- Will understand that all the settings ICT equipment is primarily intended to support management and learning and will only be used for personal or recreational use if specific permission has been given.

Buying and Selling.

- The provider will not allow others to use equipment owned by the setting for online purchasing unless it is for use by the pre school and they have been given permission to do so.

Social networking sites

- Access to social networking sites is not permitted by children and young people in the setting.
- Early years managers and practitioners are not permitted to use work related technologies for personal access to networking sites, unless it is for approved activity relating to the setting such as uploading photographs to the settings Facebook page.
- The use of these sites in adults recreational time cannot be restricted however early years managers and practitioners must adhere to our professional conduct agreement. Content which may compromise professional integrity or will bring the setting into disrepute is not permissible and may result in disciplinary action.
- It is not permissible for early years managers or practitioners to engage in personal online communications with children, young people, parents or carers. This includes the use of social media networking platforms such as Facebook and Twitter. However as previously stated this can and does happen as parents make the initial contact with staff. When this happens staff should respond appropriately and politely but should also inform parents of the correct routes of contact such as the pre school mobile/landline, in person or via email.
- Any known misuse, negative and/or anti-social practices must be reported immediately to the DPS.

Problems.

- We will ensure that others understand their duty immediately to report to the provider.
- Any illegal, inappropriate or harmful material or incident of which they become aware.
- Any damage or faults involving equipment or software, however this may have happened.
- **If we believe a young person may be at risk we will follow our child protection procedures.**
- **If we believe a child or adult may be being bullied we will follow the agreed procedures.**

We will ensure that others understand their duty not to;

- Install or store programmes on a computer owned by the provider unless they have permission.
- Try to alter computer settings, unless this is allowed in this settings policies.
- Cause damage to ICT equipment in the setting.
- Open any pop-ups or attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes

Reviewed by

Manager …… Date ……..

Staff …… Date ……..

Trustees …… Date ……..