SAFEGUARDING & WELFARE REQUIREMENT CHILD PROTECTION

1.5 Acceptable Use Policy (AUP) (Pol No. 55)

Policy Statement

The Acceptable Use Policy (AUP) 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 have access to and/are users of, work related ICT systems.
- ensure all ICT users have an awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

This Acceptable Use Policy also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

Scope

The AUP will apply to all individuals who have access to and/or are users of work-related ICT systems. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, board members, visitors, contractors and community users. This list is not exhaustive.
Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that take place on-site, and, where relevant, offsite.

Roles and Responsibilities

Registered Person
The registered person has overall responsibility for ensuring that online safety is an integral part of everyday safeguarding practice.

This will include ensuring that:
- early years practitioners and their managers receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.

• clear and rigorous policies and procedures are applied to the use/non-use of personal ICT equipment by all individuals who come into contact with the early years setting. Such policies and procedures should include the personal use of work-related resources.
• the AUP is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity.
• monitoring procedures are open and transparent.
• allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies where applicable.
• effective online safeguarding support systems are put in place, for example, filtering controls, secure networks and virus protection.

Senior Designated Person for Safeguarding (SDPS)
The senior Designated Person for Safeguarding must be a member from the management team who has relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role should be available at all times, including where necessary the use of a designated deputy.

The Senior Designated Person for Safeguarding will be responsible for ensuring:
• agreed policies and procedures are implemented in practice.
• all updates, issues and concerns are communicated to all ICT users
• the importance of online safety in relation to safeguarding is understood by all ICT users
• the training, learning and development requirements of early years practitioners and their managers are monitored and additional training needs identified and provided for.
• an appropriate level of authorisation is given to ICT users. Not all levels of authorisation will be the same – this will depend on, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities where deemed appropriate.
• any concerns and incidents are reported in a timely manner in line with agreed procedures.
• the learning and development plans of children and young people address online safety.
• a safe ICT learning environment is promoted and maintained.

Early Years Practitioners and their Managers
Early years practitioners and their managers will ensure:
• the timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures (within the same day/as soon as practicably possible)
• ICT equipment is checked before use and all relevant security systems judged to be operational.
• awareness is raised of any new or potential issues and any risks which could be encountered as a result.
• children and young people are supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
• online safety information is presented to children and young people as appropriate for their age and stage of development.
• children and young people know how to recognise and report a concern.

- all relevant policies and procedures are adhered to at all times and training undertaken as required.

Children and Young People

Children and young people should be encouraged to:

- be active, independent and responsible learners, who contribute as appropriate to policy and review.
- abide by the Acceptable Use Agreement.
- report any concerns to a trusted adult.

Parents and Carers

Parents and carers should be encouraged to sign Acceptable Use Agreements and to share responsibility for their actions and behaviours.

A copy of an Acceptable Use Agreement should be provided to parents and carers on enrolment of their child at the early years setting. This will be reviewed regularly. It is an expectation that parents, and carers will explain and discuss the Acceptable Use Agreement with their child to ensure that it is understood and agreed. Children and young people will also be encouraged to sign the Acceptable Use Agreement alongside their parent or carer where appropriate. Records of all signed agreements should be kept on file.

Should parents or carers wish to use personal technologies, (such as cameras) within the setting environment, practice must be in line with the setting's policies.

Acceptable use by Early Years Practitioners, their managers and volunteers

Early years practitioners, their mangers and volunteers should be enabled to use work based online technologies:

- to access age appropriate resources for children and young people;
- for research and information purposes;
- for study support.

All early years practitioners their managers and volunteers will be subject to authorised use as agreed by the Senior Designated Person for Safeguarding (SDPS).

All early years practitioners, their mangers and volunteers should be provided with a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they must sign, date and return. A signed copy should be kept on file.

Authorised users should have their own individual password to access a filtered internet service provider. Users are not generally permitted to disclose their password to others, unless required to do so by law or where requested to do so by the Senior Designated Person for Safeguarding. All computers and related equipment that can access personal data should be locked when unattended to prevent unauthorised access.

The use of personal technologies is subject to the authorisation of the Senior Designated Person for Safeguarding, and such use should be open to scrutiny, monitoring and review.

In the event of misuse by Early Years Practitioners, the Managers or Volunteers

In the event of an allegation of misuse by an early year's practitioner, manager or volunteer, a report should be made to the Senior Designated Person for Safeguarding and/or the registered person

immediately, as relevant. Should the allegation be made against the Senior Designated Person for Safeguarding, a report should be made to a senior manager and the registered person. Procedures should be followed as appropriate, in line with the ICT Misuse Procedure, Safeguarding Policy and/or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police should be notified as applicable.

Acceptable use by Children and Young People

Acceptable Use Agreements are used to inform children and young people of behaviours which are appropriate and others which are deemed unacceptable. This will allow children and young people to take some degree of responsibility for their own actions, understanding the risks and likely sanctions.

The Acceptable Use Agreements are shared and agreed with children and young people, (where understanding is possible) and should be displayed as a reminder.

In the event of misuse by Children and Young People

Should a child or young person misuse ICT, the following sanctions will be applied:

- Step 1: In the event of deliberate misuse, the parent/carer is informed of the issue. The child or young person may be temporarily suspended from a particular activity.
- Step 2: Further incidents of misuse, could lead to the child or young person being 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 with a senior manger and the most appropriate course of action will be agreed.
- Step 3: The sanctions for misuse can be escalated at any stage, if considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. If a child or young person is considered to be 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, Children's Social Care. 7.2 In the event that 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.

The above steps apply to adults where applicable.

Acceptable use by visitors, contractors and others

All guidelines in respect of acceptable use of technologies must be adhered to by any visitors or contractors.

POLICY NUMBER 55

The policy was adopted at a meeting of……

Held on……..

Date to be reviewed…….

Signed on behalf of the provider……..

Name of signatory……

Role of signatory……