**ACCEPTABLE USE POLICY**

Aim

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/devices.

• Ensure all ICT users have an awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Scope

The Acceptable use policy will apply to all individuals who have access to and/or are users of work-related ICT systems/devices. This will include children, early years practitioners, managers, volunteers, students, committee members, and visitors. 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, off-site.

Roles and Responsibilities

**Designated safeguarding Lead (DSL)**

The DSL has overall responsibility for ensuring that online safety is an integral part of everyday safeguarding practice. They must have relevant, current, and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role should be always available, including where necessary the use of a designated deputy.

Their role will include ensuring that:

• Early years practitioners 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.

• The AUP is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity.

• Allegations or misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies where applicable.

• Effective on-line safeguarding support systems are put in place, for example filtering controls, secure networks and virus protection.

• Agreed policies and procedures are implemented in practice.

• The importance of on-line safety in relation to safeguarding is understood by all staff.

• An appropriate level of authorisation is given to all staff. 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**

• The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.

• 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 are supported and protected in their use of online technologies – enabling then to use ICT in a safe and responsible manner by using age-appropriate apps, websites and online tools.

• Online safety information is presented to children as appropriate for their age and stage of development as well as modelling safe practice.

• All relevant policies and procedures are always adhered to and training undertaken as required.

Acceptable Use by Early Years Practitioners, Managers, Volunteers and students

All the above should be enabled to use work based on-line technologies:

• To access age-appropriate resources for children.

• For research and information purposes.

• For study support.

All the above will be subject to authorised use as agreed by the Designated safeguarding Lead.

All the above will be provided with a copy of the Acceptable Use Agreement, which they must sign, date and return. A signed copy will be kept on file.

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 Designated safeguarding lead, and such use should be open to scrutiny, monitoring, and review.

In the Event of misuse by Early Years Practitioners, managers, volunteers and students

In the event of an allegation of misuse a report should be made to the Designated safeguarding lead immediately, as relevant. Should the allegation be made against the DSL, a report should be made to the deputy DSL and/or the registered person. Procedures should be followed as appropriate, in line with the safeguarding Policy and/or Disciplinary Procedures. Should allegations related to abuse or unlawful activity, Children’s Social Care, the Local Authority Designated Officer, Ofsted and/or the Police should be notified as applicable.

If a child accidentally accesses inappropriate material, it must be reported to the DSL 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 for investigations to take place.

Links to Other Policies

Safeguarding Policy

The Safeguarding Policy should be refereed to when dealing with any incidents that occur as a result of the intentional or unintentional misuse of ICT. Any allegations of abuse or other unlawful activity should be reported immediately to the DSL who will ensure procedures outlined in the Safeguarding Policy are followed with immediate effect.

Designated Safeguarding Lead is Michelle Howell/Deputy safeguarding officer is Donna Roberts

This policy was adopted at a meeting of the pre-school held on 05.07.22

Signed on behalf of the pre-school …………Gary Cox………….

Reviewed 15/08/23