NORTHLEACH PLAYGROUP

Mill End, Northleach, Cheltenham, Gloucestershire, GL54 3HJ
Registered Charity No. 1015852

Acceptable Use Policy

Statement of Intent

This policy will reference the Early Years Foundation Stage This Policy should be read in conjunction with Northleach Playgroups ICT and Data Policy, Mobile Phone and Digital Photography Policy and Safeguarding 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.
• Ensure all ICT users have an awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.
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, committee 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, off-site

Method

The DSL 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 the early years setting. Such policies and procedures should include the personal use or work-related resources (see ICT and Data Policy, Mobile Phone and Digital Photo Policy and Safeguarding Policy)
• The AUP is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity.
• Allegations, 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.

The Designated Safeguarding lead 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 on-line safety in relation to safeguarding is understood by all ICT users.
• The training, learning and development requirements of early year's 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 address online safety.
• A safe ICT learning environment is promoted and maintained.

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.
• 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 that 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.
• Online safety information is presented to children as appropriate for their age and stage of development.
• All relevant policies and procedures are adhered to at all times and training undertaken as required.
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 DSL. 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 DSL, and such use should be open to scrutiny, monitoring and review. In the Event of misuse by Early Years Practitioners, their Managers or Volunteers

In the event of an allegation of misuse by Early Years 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 appropriated, in line with the On-line Compass Flowchart, Safeguarding Policy and/or Disciplinary Procedures. Should allegations related to abuse or unlawful activity, Children's Social Care (Family Contact Point – MASH), the Local Authority Designated Officer, Ofsted and/or the Police should be notified as applicable.

Signed on behalf of the Management Committee _____

Role of signatory (e.g. chairperson etc.) _____