



NORTHLEACH PLAYGROUP

Mill End, Northleach, Cheltenham, Gloucestershire, GL54 3HJ

Registered Charity No. 1015852

E-Safety Policy

Statement of Intent

This policy details how Northleach Playgroup polices the use of ICT by staff, children, volunteers, parents, carers and visitors to ensure everyone's "e-safety".

E-Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing.

It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Additionally we require that staff uphold the setting's reputation at all times when using social networking sites.

The Internet is an essential element in 21st century life for education, business and social interaction. Northleach Playgroup has a duty to provide children with quality Internet access as part of their learning experience.

Our ICT policy will operate in conjunction with other policies including those for Safeguarding, Behaviour Management, Health & Safety, Mobile Phone, Personal Calls & Social Networking, Parental Involvement & Use of Photographs within playgroup.

Roles and Responsibilities

The Playgroup Manager has a duty of care for ensuring the safety (including e-safety) of the children, staff and volunteers of Northleach Playgroup.

The Playgroup Manager has overall responsibility for ensuring the online safety is an integral part of everyday safeguarding practice.

The Playgroup Manager and Deputies are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart appendix on dealing with e-safety incidents)

The Playgroup Manager ensures:

- All staff 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 setting.
- Such policies and procedures include the personal use of work-related resources.
- 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.

Aims

- To safeguard children and young people by promoting appropriate and acceptable use of information and communication technology (ICT)
- To enable all children to build on their experiences from home
- To enable all children to develop practical skills needed to access ICT
- To enable all children to enjoy ICT and use it with confidence
- To enable all children to understand that equipment needs to be handled with care and respect.
- To ensure all children can use ICT as a tool for collaborative decision making and conversation
- To ensure all children can listen to and understand instructions
- To ensure all children can problem solve and think logically to complete tasks.
- To enable staff to improve their skills and confidence in the use of ICT to promote children's learning.
- To enable parents to improve their confidence in the use of ICT to support their children's learning.
- To outline the roles and responsibilities of all individuals who have access to and/are users of work related ICT systems
- To ensure all ICT users have an awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

How we use ICT

ICT has become part of the way in which we all work and entertain ourselves.

A great deal of activities in Playgroup now involve the use of ICT:

- online activity research, teaching plans and resource materials;
- activity delivery via the interactive whiteboard;
- communication by e-mail;
- document distribution and storage;
- assessment information analysis;

Thus, through teaching ICT, we equip children to participate in a world of rapidly changing technology. We enable them to find, explore, analyse, exchange and present information. We also help them to develop the necessary skills for using information in a discriminating and effective way. This is a major part of enabling children to be confident, creative and independent learners.

To ensure that quality of care is never compromised through use of ICT. Responsible use of ICT is to be encouraged by education and explicit in our policy. To uphold the setting's reputation through staff's and committee's interaction with and use of ICT within the setting and beyond.

Safe and secure broadband which ensures the effective management of filtering.

Staff

are responsible for ensuring that:

- they have an up to date awareness of ICT & e-safety and of the Playgroup's ICT policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they ensure children have regular access to equipment in order to improve the quality of learning.
- they ensure there is specific software that may be beneficial to children with SEN
- they seek professional development as part of their training to support children's learning through the use of ICT in order to raise achievement to fulfil the EYFS.
- they report any suspected misuse or problem to the *Playgroup Manager/ Deputy* for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- children parents & carers understand and follow the ICT and acceptable use policies
- they provide opportunities for parents to work alongside their children on ICT activities

Our Designated Safeguarding Lead is trained in e-safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Managing Internet Access/Online safety

It is essential that children are safeguarded from potentially harmful/inappropriate online material.

Four areas of risk:

Content - exposed to illegal, inappropriate or harmful content. eg: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

Contact - subjected to harmful online interaction eg: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and exploit them for sexual, criminal, financial or other purposes.

Conduct - personal online behaviour that increases the likelihood of or causes harm eg: making, sending and receiving explicit images.

Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Safe use of the Internet

How will Internet use provide effective learning?

- Staff, parents and children need to develop good practice in using the Internet as a tool for teaching and learning
- The setting will work in partnership with parents and the Internet Service Provider to ensure systems to protect children are reviewed and improved for safe use at all times
- Children will be monitored and supervised appropriately at all times whilst accessing the Internet
- Internet access will be planned to enrich and extend learning activities
- Only those children who have received written permission from parents/carers will be able to access information via the Internet
- The setting will ensure that written permission will be actively sought and information provided to parents/carers will be relevant, detailed and informative
- The Playleader will ensure that regular checks are made to ensure that the filtering methods in place are effective
- Virus protection will be installed and updated regularly

E-mail

- E-mail sent to an external organisation should be written carefully

Published content and the Playgroup web site

- The contact details on the Web site is the Playgroup address, e-mail and telephone number. Staff or children's personal information will not be published.
- The Committee and manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual children to be clearly identified.
- Children's full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school Web site.

Social networking and personal publishing

- We will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Parents will be advised that the use of social network spaces outside school is inappropriate for Early Years children.
 - Staff/committee must not post anything onto social networking sites such as "Facebook" that could be construed as having an impact on the setting's reputation.
 - Staff/committee must not post anything onto social networking sites that would offend any other member of staff or parents/carers using the setting.
 - If staff/committee choose to allow parents/carers to view their page on social networking sites, then they must not refer to playgroup or their role with playgroup.

Managing filtering

- Northleach Playgroup will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Playgroup Manager

Mobile Phones

Northleach Playgroup has drawn up a Mobile Phone, Personal Calls and Social Networking Policy, which is outlined below.

- Personal calls will not be accepted through the main setting's phone line unless in an emergency situation.
- The setting's number may be used and given out as a contact point for emergency calls.
- Mobile phones are not to be turned on during working hours unless required for work purposes.
- Mobile phones must not be used by staff unless on a designated break time - "lunch" and then it must be away from children unless for work purposes.

- Mobile phones should be stored safely away in staff's personal bags at all times during working hours.
- On arrival at the setting all parents/carers/visitors that will be staying at the setting during a session are asked to surrender their phones to ensure the children's safety.
- Staff, committee and other parents/carers are not allowed to take photos of the children using their mobile phone.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any Playgroup ICT resource.
- Parents will be asked to sign a Child's Acceptable ICT use Agreement, which informs them of our policy and use.
- Playgroup will keep a record of all staff and children who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Assessing risks

- Playgroup will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a playgroup computer. Playgroup cannot accept liability for the material accessed, or any consequences of Internet access.
- Playgroup will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse by children or staff will be dealt with by the Manager and Chairperson of Northleach Playgroup Committee. A complaint against the Manager must be addressed to the Chairperson.
- Complaints of a child protection nature must be dealt with in accordance with the playgroup's child protection procedures.

Communications Policy

Introducing the e-safety policy to children:

E-safety rules will be posted in the setting and discussed with the children regularly

Staff

All staff will be given the ICT and Acceptable Use Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the Playgroup's ICT and Acceptable Use Policy in newsletters, prospectus and on the setting's Web site.

If a member of staff or committee member should know of, or become aware of any breach of the code of conduct by another member of staff or committee, they are obligated to notify the Playleader.

Breaches of the code of conduct may also be brought to the attention of the Committee by staff and non- staff members.

If any of the above points are found to be happening then the member of staff or committee that is involved will face disciplinary action, which may result in dismissal.

Signed on behalf of the Management Committee _____

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