Milborne Ladybirds Playgroup

INTERNET SAFETY POLICY

The aim of the Internet Safety policy is to outline safe and effective practice in the use of the internet and social media.

The policy applies to all individuals who have access to ICT (Information and Communication Technology) systems in the workplace or elsewhere. This includes children, parents, carers, Early Years practitioners, volunteers, students and Committee members.

The Internet Safety policy applies to internet access through any medium: - computers, laptops, tablets, mobile phones and gaming devices.

All information retained on ICT equipment is regulated according to Data Protection legislation.

Children will be protected and adults will be supported in their use of online technologies, enabling them to use ICT in a safe and responsible manner.

Children and adults will be helped to recognise and report a concern

Responsibilities

The senior Designated Safeguarding Lead and the Deputy Safeguarding Lead are responsible for online safety and implementation of this policy.

The designated person for online safety will:

- Be responsible for online safety issues and as such will have the leading role in implementing, monitoring and reviewing the Internet Safety policy.
- Inform all ICT users of the procedures that must be followed in the event of a potentially unsafe or inappropriate online incident taking place.
- Maintain records, monitor and file reports in the event of a potentially unsafe and inappropriate online incident.
- Take all necessary actions to minimise the risk of any unsafe or inappropriate online incidents occurring.
- Check before use that all ICT equipment has the appropriate security systems and that they are operational.
- Raise awareness of any new potential issues and any risk which could be encountered as a result.
- Undertake any necessary training in order to remain up to date with current legislation and best practice

The designated persons for Internet Safety are –
Liz Dyer (staff)

Managing online access

- All computers, laptops and tablets should have password protection. Access to personal information must have separate password protection specific to the individual child.
- A list of authorised ICT users should be maintained and access to sensitive personal data must be restricted.
- Computers and laptops should have "timeout" settings so if they are inadvertently left on they cannot be accessed by an unauthorized person, all ICT users must log out of their accounts on completion of the task.
- If users become aware that passwords have been compromised, they must inform the designated internet safety person in order to change them promptly.
- As Ladybirds do not have a central computer there will be times when it is necessary to transfer data between computers. Any memory device used for this purpose will be a designated for sole use by Ladybirds and once the information has been transferred the data on the device will be deleted from that device.

Internet access

Internet access for all ICT users should be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution should be taken to ensure the safe use of the internet.

The following control measures must be in place where appropriate to minimize the risk:

- Secure broadband or wireless access
- A secure, filtered and managed internet provider
- Secure email accounts
- Regularly monitored and virus protected
- Password system
- An agreed list of assigned authorized users
- Effective audit and monitoring process.
- Devices for children's use must be in high visibility areas which will enable children and adults to be closely supervised and their online use appropriately monitored.

Reporting incidents

If a child accidently assesses inappropriate material, it must be reported to an adult immediately. Appropriate action should be taken to hide; minimize the window; the computer should not be turned off; the page closed, in order to allow investigations to take place.

All such incidents must be reported to the designated internet safety person.

Online communications

- All official online communication must occur through secure filtered email accounts.
- All ICT users are expected to write online communications in a polite, respectful, and non-abusive manner.

- Communication between adults and children should take place within open, impersonal and professional manner. This includes the wider use of technology such as mobile phones, text, social networking, email, web-cams, websites and blogs.
- When using digital communications staff and volunteers should only make contact with children/ young adults for professional reasons
- Personal information must not be shared with children
- All communications must be transparent and open to scrutiny
- Social networking profiles held by any adult employed or volunteering with the preschool must not be shared with children in their care making every effort to keep personal and professional online lives separate.
- Staff must not post information online that can bring the setting into disrepute
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Managing mobile phone and emerging technologies

Emerging technologies should be valued for learning and development opportunities they provide for children. Many of these technical devices will be equipped with internet access:- GPS, cameras, video and audio recordings, they must therefore be considered subject to the same control measures above to minimise risk

Early Years practitioners and Committee members are likely to use social networking sites in their own time on their own computers, this form of activity is not discouraged however they must agree to adhere to a professional conduct agreement, the use of these sites should not compromise professional integrity or bring the preschool into disrepute. The adding of "friends" of children and parents of the setting should be avoided.

Images

All images will be used in the manner that meets the principles of Data Protection, this is:-

- Fairly and lawfully processed
- Processed for specifically stated purposes
- Used in a way that is adequate and relevant
- Accurate and up to date
- Kept on file for no longer than is necessary
- Processed in line with individuals rights
- Kept securely

In the event of misuse by Early Years practitioners, volunteers or Committee members

- In the event of an allegation of misuse a report will be made to the designated person for internet safety
- Should the allegation be made about the designated person a report should be made to the Management Committee.
- Procedures will follow the preschool's Disciplinary policy.

- Should allegations relate to abuse or unlawful activity children's social care, the local authority, Ofsted and the police will be informed.

Reviewing the Policy

The Internet Safety Policy will be kept under review and will be reviewed annually.
This policy was agreed at a meeting of the Management Committee held on 25 August 2020

Signed ……………………………………………….. Chairperson