Little Owls
PRE-SCHOOL

Acceptable Use, Online/E-Safety Policy

Little Owls Acceptable Use Policy

Version Control Log

Date	Date agreed with Managers	Overview of changes
January 2019	January 2019	Review and update policy

Introduction

Information Communication Technology (ICT) and the Internet have become an integral part of our modern lives and helps provide our children, staff and parents/carers with opportunities to improve communication, understanding and to access resources quickly. This policy comprises legislation (Keeping Children Safe in Education, 2018) and good practice as outlined in the Online Safety Toolkit.

The following list identifies common internet-based technologies, which are likely to be used by children either at home or in an educational context:

Websites and the use of apps (on a variety of devices);

Social Media, including Facebook and Twitter; Web-enabled mobile/smart phones;

Online gaming;

Learning platforms and Virtual Learning Environments;

Video broadcasting;

Blogs and Wikis; E-mail,

Instant messaging, chat rooms and chat forums.

Whilst the majority of the children at Little Owls are unlikely to have been introduced to most of these applications/services, some may already be using them individually, whilst others will almost certainly have experienced parents/carers or older siblings using them. As such, we must continue to introduce our children to ICT whilst promoting safe use of online technologies, both within Little Owls and their home environment.

The term ‘online safety’ is taken to mean the safe and appropriate use of all web, mobile or networkbased information, communication and storage technologies.

The term ‘e-safety’ refers to the safe use of all electronic technologies, which may or may not be used with the internet, in order to protect users (children and adults) from potential and known risks.

We will help our children to learn how to consider and moderate their own behaviours when using technology and begin to understand how to recognise inappropriate and unsafe behaviour in other users. Thus, it is vital that there are clear rules, procedures and guidelines to minimise risks whilst children use these technologies. Such risks include:

Commercial issues with spam and other inappropriate e-mail;

Grooming by people who may abuse children, usually someone pretending to be younger than their true age;

Illegal activities of downloading or copying any copyright materials and filesharing via the Internet or any mobile device;

Viruses;

Cyber-bullying;

Accessing on-line content, either deliberately or accidentally, which is abusive, offensive or pornographic.

At Little Owls we have a duty to ensure that our children are protected from potential harm both within and beyond Little Owls. However, it is likely that we will never be able to completely eliminate risks and any incidents that do arise will be dealt with quickly and in accordance with our policy.

Aims of the Policy

The aims of this policy can be summarised as follows:

- To safeguard children and young people by providing rules and promoting appropriate and acceptable use of ICT and the internet;
- To outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT and internet systems;
- To ensure all ICT users have an awareness of risk, a clear understanding of what constitutes misuse and the process and sanctions that may be applied;
- To develop links with parents/carers.

Purpose of the Acceptable Use Policy

This Acceptable Use Policy:

Clearly sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard the children and adults within Little Owls;

Outlines the steps taken within Little Owls to facilitate online/e-Safety of our children when using the internet and other related technologies;

Outlines Little Owls' expectations for the behaviour of the children, staff, parents/carers, visitors, volunteers, Trustees whilst using the internet and related technologies within, and beyond, Little Owls.

Acceptable Use - Protocol, procedures and sanctions

Adult Responsibilities

All adults (staff or volunteers) have a shared responsibility to ensure that our children are able to use the internet and related technologies appropriately and safely. All adults that work or volunteer in the setting are required to read and comply with our policies and procedures.

All our policies and procedures are accessible to visitors, parents/carers and are applicable to all.

All adults must take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected

- the device must be password protected
- the device must have virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete.

Early years practitioners and their managers will be responsible for keeping their passwords secure and must ensure they are to be regularly up-dated.

Sharing passwords is not to be considered secure practice. Where children and young people are to be enabled to create their own password however, a copy of such will be kept on file for reference.

It is to be considered good practice for computers and laptops to be set to 'timeout' the current user session should they become idle for an identified period. All ICT users must 'log out' of their accounts should they need to leave a computer unattended.

If ICT users should become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the Designated Safeguarding Lead.

All official online communications must occur through secure filtered email accounts and communications will be expected to be written in a polite and professional manner.

A filtered internet server is to be used to monitor and prevent offensive material or spam. Should, on rare occasions, security systems not be able to identify and remove such materials, the incident will be reported to the Designated Safeguarding Lead.

The Designated Safeguarding Lead has overall responsibility for online/e-safety with the Deputy Designated Safeguarding Lead having day-to-day responsibility. Together, they:

Help ensure all employees, volunteers, parents/carers are aware of Little Owls responsibilities relating to online/e-safety;

Help ensure all staff comply with the policies and procedures;

Help establish and maintain a safe ICT learning environment e.g. via safe and secure emails, filtered internet, antivirus software, etc.

Help ensure relevant Policies and Procedures are updated as/when required and staff, volunteers and Trustees are briefed and/or trained accordingly;

Help promote online/e-Safety awareness across the seven areas of learning as set out in the Early Years Foundation Stage guidance (2012);

Help ensure any equipment, which holds sensitive or confidential information and leaves Little Owls (e.g. iPads, staff laptops and memory sticks) is fully encrypted and/or password protected;

Report, and record, issues of concern and agrees any action plan, as appropriate, with the Manager, Trustee responsible for Safeguarding and/or staff;

Help ensure all staff are encouraged to read and sign our voluntary Professional Conduct Agreement (see Appendix 1).

The Children

The children are responsible for:

Using the internet and ICT technologies safely within Little Owls under the direct supervision of a member of staff;

Informing adults of anything they find upsetting/inappropriate;

Being supported to understand, and follow, the children's 'Acceptable Use Rules' (Appendix 2).

Inappropriate Use – Procedure for following up incidents

In the event of staff, volunteer, Trustee misuse

If a member of staff, a volunteer or a Trustee is believed to have misused the internet or Little Owls network in an illegal, inappropriate or abusive manner, a report must be made to the Manager and/or the Trustee responsible for Safeguarding immediately. The appropriate procedures for allegations must be followed (other policies may need referring to) and the following teams/authorities contacted:

The LA Safeguarding Team;

The LADO;

Police/CEOP (if appropriate).

In the event of minor or accidental misuse an internal investigation will be initiated and staff disciplinary procedures followed if appropriate.

Examples of inappropriate use where disciplinary, safeguarding and/or police procedures may be followed:

Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

Publishing defamatory and/or false materials about Little Owls, the children, colleagues or other partners on social networking sites.

Using the internet to pursue radicalised or extremist views.

Note that steps should be taken to isolate the computer in question as best you can.

Children

In the event of inappropriate use by a child, an adult will immediately attempt to minimise or close the content and then take the necessary action.

Parents/Carers

Partnership working with parents and carers is considered good practice in the promotion of acceptable, safe online learning/E-safety.

If a parent is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, safeguarding procedures will be followed and if necessary reference will be made to protocol outlined in the Prevention of Radicalisation and Extremism Policy.

Appendix 1

Professional Conduct Agreement (copy)

We recognise that practitioners and their managers will use online and digital technologies in their personal and social lives. We do not seek to prevent any practitioner or manager from accessing online technologies however we do ask them to sign a voluntary Professional Conduct Agreement to ensure there is no confusion between their home and professional roles.

Name of practitioner/manager: ……………………………………………………………………………………………….

I agree that through my recreational use of social networking sites or other online technologies that I will:

Not bring the early years setting into disrepute □

Observe confidentiality and refrain from discussing any issues relating to work, children and young people or parents/carers □

Not share or post, in an open forum, any information that I would not want children and young people, parents/carers or colleagues to view □

Set privacy settings to block unauthorised access to my page and to restrict those who are able to receive updates. □

Keep my professional and personal life separate, and will not accept children and young people and parents/carers as 'friends' □

Consider how my social conduct may be perceived by others and how this could affect my own reputation and that of the early years setting □

Either avoid using a profile photograph or ensure it is respectable, and an image I would be happy to share with anyone □

Report any known breaches of the above □

I understand that the completion of this form is optional. However, I voluntarily choose to complete it to safeguard my own professional reputation and that of the early years setting. I understand that I am in a position of trust and my actions outside of my professional environment could be misinterpreted by others, and I am conscious of this when sharing information publicly with others.

Signature:……………………………………………………………………. Date: …………………………………………………..

Appendix 2

Children’s Computer/Internet Rules

- I will ask a grown up before I use a computer/tablet;
- I will only use activities that a teacher has told me to use
- I will take care of the compute/tablet and other equipment
- I will ask a teacher if I think I have done something wrong or I am not sure what to do
- I will tell an adult straight away if I see something on the computer that I think should not be there;
- I know these rules are there to help me, my friends and my family feel safe.