Technology and Communications Policy

Acorns 2 Oaks Ltd.(A2O) uses several different methods of electronic communication in its work and recognises that there may be occasions when employees would wish to use these systems for personal reasons. This is permitted subject to the personal usage not affecting the work of the individual, others in Acorns 2 Oaks Ltd., or the systems used.

Acorns 2 Oaks Ltd regards appropriate and safe communication as imperative to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals. This Technology and Communications Policy exists to:

- Ensure the protection and safety of children accessing their service, in conjunction with Child Protection Procedures
- Ensure the protection of the Organisation and its staff
- Uphold the principles of the Data Protection Act 1998 (revised 2000), The General Data Protection Regulations (GDPR) 2018, and the organisation's respective policy
- Maintain confidentiality in line with the organisation's respective policy

Contents

Acceptable Use and User Agreement

AUP applies to all individuals who have access to and/or are users of work-related ICT systems. This includes children, parents and carers, early years practitioners and managers, volunteers, students, visitors and contractors. Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and where known, off-site. Acorns 2 Oaks Acceptable Use Policy (AUP) aims to:

- Safeguard our children and deter any breach of data protection by promoting appropriate and acceptable use of information and communication technology (ICT).
- Outline the roles and responsibilities of all individuals who are to have access to and/or be users of work-related ICT systems.
- Ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be supplied.

Registered person

The Chief Executive and Senior Management have overall responsibility for ensuring online safety is considered an integral part of everyday safeguarding practice. This includes ensuring:

- 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 affect or come into contact with the A2O. Such policies and procedures include the personal use of work-related resources.
- The AUP is implemented, monitored and reviewed regularly, and all updates are shared with relevant individuals at the earliest opportunity.
- 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.
- Effective online safeguarding support systems are put in place, for example, filtering controls, secure networks and by encryption and virus protection.

The Designated Safeguarding Leads (DSL) are *Lauraine Nicholson, Sidra Abbas (Canterbury), Marjorie McFee* (Peppermint). The Deputies are Kelly Sloan *(Canterbury) and Bianca D'Souza (Peppermint).*

They are 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 online safety in relation to safeguarding is understood by all ICT users.
- The training, learning and development requirement of all staff is monitored and additional training needs identified and provided for.
- An appropriate level of authorisation is given to ICT users. Not all levels of authorisation are the same – this depends on, for example, 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 will address online safety.

- A safe ICT learning environment is promoted and maintained.

All Early Years Practitioners 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 which could be encountered as a result.
- Children are supported and protected in their use of online technologies-enabling them 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.
- We will endeavour to ensure that children know how to recognise and report a concern.
- All relevant policies and procedures are adhered to at all times and training is undertaken as it is required.

General procedures:

- Authorised users have their own individual password. Users are not generally permitted to disclose their password to others.
- Computers must be closed down at the end of day, allowing updates to be installed and minimising the risk of hacking.
- Software applications or updates must not be installed from either the Internet or other hardware devices without authorisation from the Senior Administrator.
- All Staff are provided with a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they must sign, date and return. A signed copy is to be kept on file.
- USB Sticks must **not be used**.
- Copies of files should be kept at work or emailed to your line manager so that they are available to other staff who need to access them.

Individuals will also be required to sign additional Acceptable Use Agreements if they are to undertake any voluntary work within A2O and/or participate on associated trips or visits. Early Years Practitioners work-based online technologies:

- To access age appropriate resources for children
- For research and information purposes;
- For study support.

ICT Misuse

The use of personal technologies is subject to the authorisation of the DSL, and such use will be open to scrutiny, monitoring and review.

- Should it be alleged, that a member of staff or manager is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report will be made to the DSL immediately.
- Should the allegation be made against the DSL a report will be made to the Deputy DSL. Procedures will be followed as appropriate, in line with the ICT Misuse Procedure, Child Protection Policy and/or Disciplinary Procedures.
- Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.
- All children will only be able to access ICT Resources with the supervision of an Early Years Practitioner. In the event that a child should accidentally access inappropriate material, appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access. This must be reported to the DSL immediately.

Acceptable use by visitors, contractors and others
All individuals who affect or come into contact with the early years setting are expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with children. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.

Links to other policies
Behaviour Policy - The Anti-bullying Policy contains up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyber bullying. It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the 'real' and 'cyber' world and this is reflected in all relevant policies.

Safeguarding Policy is to be referred 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 are to be reported immediately to the DSL who will ensure procedures outlined in the Safeguarding Policy are followed with immediate effect.

Personal, Social and Emotional Development (PSED) - The promotion of online safety within PSED activities is considered essential for meeting the learning and development needs of children and young people. Key messages to keep children and young people safe are promoted and should be applied to both online and offline behaviours.

Acceptable Use Agreement for Staff and Volunteers

Acorns 2 Oaks Acceptable Use Agreement is intended to support the online safety of the setting and individual staff and volunteers through:

- Staff and volunteers acting responsibly to stay safe while online and being good role models for younger users.
- Effective systems being in place for the online safety of all users and the security of devices, systems, images personal devices and data.
- Staff and volunteers being aware of how they can protect themselves from potential risk in their use of online technologies.

The term 'professional' is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety, I understand that:

- I should ensure that my on-line activity does not compromise my professional responsibilities, nor bring Acorns 2 Oaks into disrepute.
- My use of technology could be monitored.
- When communicating professionally I will use the technology provided by the setting (e.g. email). These rules also apply when using the Organisation's technology either at home or away from the setting.
- Personal use of the Nursery's technology is only acceptable with permission.

For the safety of others:

- I will not access, copy, remove or otherwise alter any other user's files, without authorisation.
- I will communicate with others in a professional manner.
- I will share other's personal data only with their permission.
- I will use the Nursery's equipment to record any digital and video images, unless I have permission to do otherwise from DSL

For the safety of the settings, I understand that:

- I will not try to access anything illegal, harmful or inappropriate.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident.
- I will not share my online personal information (e.g. social networking profiles) with the children in my care.
- I will not deliberately bypass any systems designed to keep the Nursery safer.
- I understand that Data Protection Policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the setting's policy to disclose such information to an appropriate authority.
- Personal passwords and those of other users should always be confidential.
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules.
- I will inform the appropriate person if I find any damage or faults with technology.
- I will not attempt to install programmes of any type on the devices belonging to the Organisation without permission.
- I have read and understand the above and agree to use the settings technology and my own devices when carrying out communications related to the group within these guidelines.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Monitoring and interception

Acorns 2 Oaks Ltd. reserves the right to monitor the use of its communications systems to ensure that it remains within the law, its usage policies are being followed, and to ensure that the systems are operating efficiently, thus:

- All calls made using A2O systems will be routinely monitored, including the number called, the number called from, and the duration and cost, but not including the content of the call.
- A2O reserves the right to record the content of some calls. In these cases the individuals will be informed that the call is being recorded.
- Email traffic will be routinely monitored, including source and destination addresses, but not content.
- All email will be checked for the presence of computer viruses. This checking will be carried out automatically and the content will not be accessed by any member of staff. Any emails found to be infected will be automatically deleted.
- In the event of a member of staff being unavailable for work due to illness or other reasons, and the information in that individual's email account is deemed necessary for the job function to be carried out, then the mailbox will be opened to the individual's line manager or their delegate. This will only be done with the written authorisation from the relevant Senior Manager or the CEO.
- Internet usage will be routinely monitored, including the sites accessed and the ID of the individual accessing them.
- Access to sites that are considered inappropriate will be blocked automatically, and such access attempts logged.

The organisation reserves the right to access information stored on the facilities it provides. However, the right will only be exercised in order to access information essential for its business purposes, e.g. during absence or to investigate a suspected breach of A2O regulations or the law, and only on the explicit authority of the relevant member of the Senior Management Team or the CEO. Such authority can be given both verbally and in written form.

Staff who fail to observe the conditions outlined in this policy may render themselves liable to disciplinary action.

Telephone Usage

A2O provides access to telephones for all staff to assist them in the performance of their jobs. It is also recognised that there may be occasions when employees would wish to use the telephones for personal reasons. This is permitted during official breaks and before or after normal working hours, subject to the following

- Personal calls should be kept as short as possible.
- Personal use of the telephones should not adversely affect the work of the individual, others in A2O, or the systems used.
- Calls to international numbers must be agreed in advance. This includes calls to mobile phones located abroad.
- Staff issued with mobile phones must only use them for **Acorns 2 Oaks Ltd** work. Any cost incurred by **Acorns 2 Oaks Ltd** for a staff member's private calls will be deducted from their remuneration.
- Wherever possible, Staff should only use the handsets designated to their department.

Telephony Protocol

Staff are requested to ensure:

- Whilst taking telephone messages they ask the caller's name and contact number and who the caller wished to contact
- Upon taking calls on behalf of others, the message and contact details are passed on to the respective colleague
- To state their name, contact number and extension when leaving voicemail messages

Emails

Acorns 2 Oaks Ltd. has provided the email system to assist employees in the performance of their jobs. It is also recognised that there may be occasions when employees would wish to use the email system for personal reasons. This is permitted subject to the following considerations, which apply to all use of the email system, whether for business or private purposes.

- All email correspondence on behalf of Acorns2Oaks must be done using the Acorns2Oaks email accounts provided.
- Line managers have access to view the staffs A2O emails, if necessary (e.g. staff absence)
- Acorns2Oaks email accounts are for business purposes only.
- New email addresses should be requested in writing/email by the line manager of the staff member.

Protection for Acorns 2 Oaks Ltd.

- The system may not be used for the exchange of messages concerning illegal activities.
- The system may not be used for personal financial gain
- Use of the system by an individual should not have a noticeable effect on the availability of the system to other users.
- Personal use of email and other computer systems should not be to the detriment of the individual's normal work activity.

Protection for A2O Staff

- The person logged in will be considered to be the author of any messages sent from that PC. Staff should always log out or lock the PC when they are away from their desks.
- Staff should not disclose their passwords to anyone else. It is also advisable to change passwords on a regular basis
- Individual email addresses should not be disclosed *unnecessarily.*

Email Protocol

The following protocols have been agreed for the use of email in Acorns 2 Oaks Ltd.:

- Messages should only be sent to those people for whom they are relevant
- The heading should clearly explain the subject of the message
- Staff should use the various email facilities enabling them to prioritise the emails they send and the "out of office" response to messages received whilst they are away
- Delete any unwanted emails regularly
- Do not open any unrecognised attachments, or any attachments from a sender you do not recognise. They may contain viruses that could damage the information on your machine and infect others.

Personal Usage
Staff may only use personal non Acorns2Oaks email account for Acorns2Oaks correspondence in the following cases:

- Lodging complaints about their line manager to their line manager, which are to must be sent to the manager's Acorns2Oaks email address.
- The Acorns2Oaks accounts are unavailable due to technical problems and the message is urgent. In this event Staff are requested to copy in their A2O email address.
- Making purchases on behalf of Acorns2Oak using their own personal credit card and/or their existing online account (e.g. Amazon). Should purchases be made on behalf of Acorns2Oaks, the Invoice or receipt must be passed to the Senior Finance Administrator for reimbursement, in line with the Finance Policy.

Internet Usage
A2O provides access to the Internet for all staff to assist them in the performance of their jobs. It is also recognised that there may be occasions when employees would wish to use the Internet for personal reasons. This is permitted during official breaks and before or after normal working hours, subject to the following considerations, which apply to all use of the Internet, whether for business or private purposes.

Protection for A2O
- Messages which may bring A2O into disrepute or which a reasonable person may consider to be offensive or abusive must not be posted on any Internet message board or other similar Web-based service. As part of routine security measures, all sites visited will be centrally logged and monitored. (Staff should note that even though you may not leave your name, other identification methods exist, including the address of the computer you are using, which may allow others to locate the organisation you work for and the particular computer used to post the message.)
- Staff must not engage in any illegal activities using the Internet.
- Inappropriate use of the internet, especially to access personal social networks, pornography or gaming is expressly forbidden.
- Individual use of the system should not have a noticeable effect on the availability of the system to other users. Staff may not participate in on-line games or have active any web channels that broadcast frequent updates to their PCs.
- The Internet may not be used for personal financial gain (including share trading).
- Web sites which display material of a pornographic nature or which contain material that may be considered offensive or illegal must not be visited. It is recognised, however, that such material may be viewed accidentally from time to time. If this happens, staff should contact the SMT immediately as the server system automatically keeps a record of the images seen and the web sites visited by all staff and students. Please bear in mind that in the eyes of the law even causing such images to be displayed, i.e. opening them, is illegal and can result in prosecution of the individual.
- Software applications or updates must not be installed from either the Internet or other hardware devices without authorisation from the Senior Administrator.

Protection for A2O Staff
- The person logged in will be considered to be the author of any messages sent from that PC. Staff should always log out or lock the PC when they are away from their desks. Under no circumstances should staff send emails from a PC which they have not logged into.

- Staff should not enter their email address on a web site unnecessarily. If staff give their address when filling in surveys or other questionnaires, they will be at risk of receiving unwanted junk messages. Colleagues' email addresses should not be disclosed without their prior consent.
- Personal information such as credit card numbers and bank account details should not be disclosed unless staff are sure that the web site is using appropriate security systems.

Social Networking

Acorns 2 Oaks regards the safety of children paramount within the settings. In conjunction with Child Protection Procedures and guidelines the sharing of information or digital images via social networking site is prohibited. Staff are prohibited from having or adding existing parents of children accessing services to a social networking site e.g. Facebook, Twitter.

- Staff members will be informed of this procedure during the staff induction.
- Child/parent confidentiality must be adhered to at all times.
- Staff with access to a social networking site will not share information about a child attending or previously attending the group
- No photographs or videos will be displayed on such sites of any child past or present at the group.
- Staff are advised not to advertise the name of the setting on such site e.g. in employment details
- Staff must refrain from stating they work in early years to prevent undesirables from infiltration any information.
- Images of the settings logo or uniform are not to be displayed in personal photographs on any social networking site.
- Staff are not to discuss any aspects of their working life as a statement or comment regarding their working day e.g. had a bad day at work child A cried all day.
- Facebook is only to be accessed via the works computer in conjunction with the groups own site.

Mobile Phones

Acorns 2 Oaks will prohibit mobile camera phones and their use in the playrooms while children are present in the setting by enforcement of the following procedures:

- Personal mobile phones will be kept in the staff locker during working hours.
- If staff need to use or check mobile phones during lunch time this must be carried out, outside the playrooms
- With permission of the manager mobile phones may be kept in the office and urgent calls maybe taken in the office only.
- ***Staff are not permitted to wear Apple Watches or Fit Bit watches that have functions to take photos or read messages during working hours***
- The main telephone number should be given to schools, family, and friends or for appointment purposes to ensure an important message is received to the recipient.
- If removing your phone from the office it must be taken through a room that does not contain children.
- Any staff member found with a mobile phone in the playrooms during opening times will be subject to disciplinary procedures and written warning will be given.
- The manager would then report the incident to the Police, OFSTED, and the Committee.

- Visitors and Professionals visiting the group will be asked to refrain from using/taking calls on their mobiles while in the playroom. They will be asked to leave the playroom if they need to take an important call.

Hard Copy Documents

- Memos are for Internal communication only
- Memos and letters should be in concise and informative form.

Clarion Call System

Clarion Call enables the organisation to send out text messages to parents, staff and trustees.
In line with Data Protection requirements, as per the Clarion Call Procedures, the use and maintenance of the Clarion system is limited to these specific personnel:

Action	Personnel
Request & Authorise Message	SMT
Send Message	SMT, Nursery Administrators
Maintain Clarion & Database	Company Secretary

Communication with the Press

A2O may need to communicate with the press from time to time, for the purposes of marketing and public relations. The objective of this policy is to clarify lines of communication between the Press and A2O. The work undertaken by A2O is of direct interest to the local community and from time to time may be reported in the press. Sometimes the press may highlight an issue that is being considered by A2O or that should be picked up by A2O.

Protection for A2O

- The Board of Trustees continually seeks to develop a more open and transparent debate to accompany our corporate decisions based on consensus amongst trustees whenever possible.
- The Board of Trustees' position is as stated in the minutes and in formal statements issued by the Board of Trustees on headed paper.
- Where the Board of Trustees is being discussed in the press, we would welcome the opportunity to respond to ensure a balanced approach and that the public are being properly informed of The Board of Trustees' position.
- Those seeking The Board of Trustees' position should approach the CE in the first instance who will put them in touch with the Chair of the Trustees.
- From time to time the CE will issue Press releases and Newsletters regarding the work of The Board of Trustees

Protection for A2O Staff

- Staff must refrain from making any public statement, written or verbal, in response to specific incidents or crises without authorization from the Chief Executive or the Board of Trustees.
- All marketing and PR releases will need to be approved by the CE and/or the Board of Trustees prior to being released

A copy of this policy can be obtained from the Nursery Offices or downloaded via our website: www.acorns2oaksnurseries.net/home/policies

Reviewed by: Beverley Noble	**Signed:** 	**Date:** Sept 2021 Review: Sept 2022