E-Safety Policy

E-safety concerns safeguarding children, young people and staff in the digital world. E-safety emphasises learning to understand and use new technology in a positive way.

Policy statement

Oasis Childcare Centres have a commitment to keeping children safe and healthy and the E-Safety Policy operates at all times under the umbrella of the Safeguarding Policy in relation to electronic communications of all types. The policy will help support and protect children, young people and staff when using technology in the settings. Every effort will be made to safeguard risks; however, it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

To ensure that our online safeguarding practice is in line with statutory requirements and best practice we refer to 'Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations for Managers (2019)' and 'Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Guidance for Practitioners (2019)'.

Scope of policy

This policy applies to all staff, children, parents/carers, committees, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of devices brought onto the premises or devices used by staff or individuals for off-site use such as a work laptop, iPad, tablet or mobile phone.

Introduction

Education on risk and responsibility is part of the duty of care that applies to everyone working with children. All staff need to understand the significance of e-safety and the importance it places on the safe use of information systems and electronic communications.

Responsibilities

Practitioners (including volunteers):

The internet is an unmanaged, open communications channel. All staff need to protect themselves from legal challenge and ensure they work within the boundaries of professional behaviour. They must ensure that they:

- Comply with current legislation

- Use the internet in an acceptable way
- Do not create unnecessary business risk to the Oasis by the misuse of the internet

Employees and professional visitors have access to wireless internet services within the setting. Access to the internet is password protected. Its content is filtered using a Draytek router which is set-up and configured by IP Office Solutions who provide our filtering and firewall service. Everyone who accesses the internet is expected to follow our E-Safety Policy, including Acceptable Use Policy. Anyone who is found to be in breach of these guidelines will be immediately denied access to our internet services. In the event of a concern being identified safeguarding procedures will be followed.

Staff must not connect any personal devices, i.e. mobile phones, cameras, smart watches, IPad's or laptops, to the settings WiFi.

In particular, the following is deemed unacceptable use of behaviour of staff:

- Visiting sites that contain obscene, hateful, pornographic or otherwise illegal material
- Using the internet to send offensive or harassing materials to others

Inappropriate use of any telephone, mobile, internet or networking site can have a negative impact on staff productivity and the reputation of the Oasis. Where it is believed that a staff member has failed to comply with this policy, they will face Disciplinary Procedure. Please see Disciplinary Procedures.

Please see attached Acceptable Use Policy for further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email or related technologies within and beyond the early years setting. A copy of this policy is available on the website and shared with any volunteers, students, parents or committees.
Office/Technical Staff:

- Anti-virus software is installed and maintained on all setting machines and portable devices
- Office computers are password protected and the passwords are changed regularly
- Access to the network is also password protected
- Any problems or faults should be reported to Designated Person for Safeguarding and recorded on the E-Safety Incident log

All staff and Management Committee regularly review this policy and it is distributed to all groups and other professionals who use the centre.

Reporting online safety concerns

The Designated Safeguarding Lead's (DSL's) take lead responsibility for online safety concerns. In the event of a member of staff having an online safety concern about a child they will promptly complete the Internal Concerns Referral Form, accurately recording the event(s) giving rise to the concern, noting dates and times, and then immediately share this information with a member of the Designated Safeguarding Team. The DSL will share the concern with the parent or guardian if this does not put the child or DSL at risk. In cases where the DSL has reason to be concerned that a child may be subject to ill treatment, neglect or other forms of abuse they have no alternative but to make a referral to the Cornwall and Isles of Scilly Safeguarding Children Partnership in writing within 48 hours. Please see Child Protection/Safeguarding Children Policy.

Depending on the nature of the concerns, the DSL would follow up the concern accordingly with the correct support body:

- Local MARU for safeguarding concerns about a child (0300 1231 116 or 01208 251300).
- The Internet Watch Foundation (IWF) to report illegal images/child sexual abuse materials: www.iwf.org.uk
- The Child Exploitation and Online Protection Centre (CEOP) if they are worried about online abuse or the way that someone has been communicating online: www.ceop.police.uk/safety-centre/
- The UK Safer Internet Helpline for Professionals (0344 381 4772) or the NSPCC (0808 800 5000) for further information.

E-Safety Support

Aaron Wilson is the Centre's Technology Consultant. He runs his own business which supports schools and settings across Cornwall, and he has over 15 years' experience in the Ed Tech environment supporting Nurseries, Schools, Colleges and Universities. Aaron has helped to bring our centre into the latest digital age; updating systems and the way we work to reduce admin time; and helping us grow and support the learning of our children. He offers onsite visits/support every fortnight and has a current DBS check in place.

Aaron provides a wealth of knowledge and support with maintaining our ICT systems and internet safety. He is instrumental at supporting us with maintaining secure internet connections and ensuring we comply with current GDPR guidelines and E-Safety regulations. Aaron provides a very professional and friendly service and offers his support to staff via email, telephone, onsite visits and remote access to our PC's. Aaron is always very prompt at responding to any issues and also offers parental support and guidance through attendance

at our regular parents evenings/days, working with staff to create displays/compile information leaflets for parents/carers and offering appointments for parents/carers to discuss individual ICT support during his fortnightly visits.

Out of Hours

A member of Senior Management will monitor all meetings held on premises, including those that happen out of opening hours.

Internet safety for children

The children in the settings do not have free access to any internet enabled devices in the Learning Rooms. Any computers that the children have access to in the Learning Rooms are not connected to the internet, with the exception of the interactive whiteboard. The interactive whiteboard must always be used under the support and guidance of a staff member.

All apps, websites and internet searches must be checked by Aaron Wilson, our Technology Consultant, and discussed with the Manager/Deputy Manager before using them with the children.

Kids Club - Homework Club

At Oasis we offer a homework club for those children who attend the after school club. There may occasions where children are required to use the internet and/or settings tablets to complete their homework tasks. Our Technology Consultant has linked the settings tablets to ClassDojo, Ludgvan School's secure platform, and children must be supervised at all times when using the tablets to complete homework tasks.

Email

The setting provides all staff with access to an individual professional email account to use for all work relating business, including communication with parents and carers. This allows for email content to be monitored and protects staff from risk of allegations, malicious emails or inappropriate contact with children. Staff must not engage in any communication with children who they have a professional responsibility for (or former pupils) via their personal email accounts.

Laptops/iPads/Tablets

Staff use:

- ICT equipment issued to staff is logged in and out

- Where staff have been issued with a device (e.g. laptop) for work purposes, personal use whilst off site is not permitted unless authorised by the Senior Manager/Senior Deputy Manager
- Staff will ensure that the settings' laptops are made available as necessary for anti-virus updates and routine monitoring
- Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless passwords have been applied

Children's use:

- Any personal gaming device, laptop, iPad or tablet with a camera is not allowed into the Learning Rooms and this is reiterated in our "Policy for The Taking of Images"

Data storage and security

Any information that is stored on the settings internet cloud storage/computers will be held in accordance with the GDPR. All staff have individual logins for the main computers and cloud storage, with a hierarchy of access to the relevant information and data for their role. All documents that contain sensitive information are password protected and access to these files is restricted to the relevant members of staff. The settings internet access is password protected and the password is only shared with relevant staff and professionals. The setting's internet network is protected by firewall systems provided by IP Office Solutions (please see Data Protection Policy).

Sensitive data, photographs and videos of children are not stored on setting devices which leave the premises such as laptops, mobile phones, iPads or USB memory sticks unless encryption software is in place.

This E-Safety Policy operates in conjunction with our other policies including the "Data Protection Policy", "Taking of Images Policy", "Child Protection - Safeguarding Policy" and the "Social Networking Policy".

Working in partnership with parents

Parents are key in keeping their children safe and still having fun in a brave, new, connected world.

Parents and carers play a vital role in supporting children to learn about how to stay safe online, and they are one of the first people children turn to if things go wrong. The following four steps are a guide to parents in supporting children in learning to be safe online as it can be difficult to stay on top of the wide range of sites and devices that young people use.

1. Have ongoing conversations with your children about staying safe online

2. Use safety tools on social networks and other online services e.g. Facebook privacy settings
3. Decide if you want to use parental controls on your home internet
4. Understand devices and the parental control tools they offer in our Parent's Guide to Technology at www.thinkuknow.co.uk/parents/parentsguide or www.getsafeonline.org.uk

The CO:RE 4Cs of online risk

The CO:RE 4Cs classification recognises that online risks arise when a child:

- Engages with and/or is exposed to potentially harmful **Content** (child as recipient).
- Experiences and/or is targeted by potentially harmful **Contact** (child as participant).
- Witnesses, participates in and/or is a victim of potentially harmful **Conduct** (child as actor).
- Is party to and/or exploited by a potentially harmful **Contract** (child as consumer).

The risks that children may be exposed to when using the internet will vary depending on their age and online activities. For many children in the early years 'Content' poses the greatest risk as young children are more likely to be at risk from what that they see or hear whilst online. However, we are mindful to ensure that each of the 4 risk categories are highlighted and shared with staff, children and parents/carers to ensure that everyone develops a good understanding of how to stay safe online.

For further information please visit:
https://core-evidence.eu/updating-the-4cs-of-online-risk/

Some useful and informative websites:

www.saferinternet.org.uk/about/helpline (more information about the helpline)
www.swgfl.org.uk/home
www.boost.swgfl.org.uk/home.aspx
www.360safe.org.uk
www.onlinecompass.org.uk
www.swgflstore.com

Adopted by The Oasis Management Committee on: 08.08.2023
Representative of Management Committee Signature: Lorna Trudgeon
Review Date: August 2024

Acceptable Use Policy

ICT and related technology such as email, the internet and mobile devices are an expected part of our daily working life. This policy is designed to make sure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its content. If you have any concerns or need clarification you can talk to the Senior Manager/Senior Deputy Manager

- I will comply with the Oasis Childcare Centres' E-Safety Policy
- I understand that using the setting's ICT system for a purpose not permitted by the Oasis may result in disciplinary or criminal procedures. Please see Disciplinary Procedures.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Administrator or the Senior Manager
- I understand that I am responsible for all activity carried out under my username
- I will only use the setting's email and/or internet for professional purposes
- I will only use the approved secure email system for any setting business
- I will not install any hardware or software without the permission of the Senior Manager/Senior Deputy Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I understand that my use of the internet and other related technologies can be monitored and logged and be made available, if requested as part of any investigation
- I will respect copyright and intellectual property rights
- I will only take, store and use images of children, young people or staff for professional purposes in line with the setting's policy and with written consent of the parent, carer or staff member. I will not distribute images outside the setting without the permission of the parent/carer, member of staff or manager
- I will make sure that my online activity both inside and outside the setting will not bring my professional role and the setting reputation into disrepute. I understand that disciplinary or legal action could be taken if I post something online which brings my professional role and/or the setting into disrepute.
- I will support the setting's e-safety policy and help children to be safe and responsible in their use of ICT and related technologies
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead or Senior Manager

- I understand that sanctions for disregarding any of the above will be in line with the setting's disciplinary procedures and serious infringement may be referred to the Police.

The following points apply in the event of staff and Committee Members having to complete virtual training/meetings in the home environment due to Covid-19:

- I will ensure that if/when I am required to complete virtual training and/or meetings in the home environment that my device is placed in an appropriate area, for example not in the bedroom, and will ensure that the background does not compromise personal confidentiality.
- I will ensure that myself and anyone else in the household are dressed appropriately.
- Language MUST be professional and appropriate at all times during the training or meeting, including any family members in the background.

I agree to follow this code of conduct and to support the safe use of ICT throughout the setting:

Full Name: _____ (printed)

Job Title: _____

Signature: _____

Date: _____ / _____ / _____

Adopted by The Oasis Management Committee on: 08.05.2023

Representative of Management Committee Signature: Lonna Trudgeon

Review Date: August 2024

E-Safety Incident Log

Details of ALL E-Safety incidents to be recorded by staff and monitored monthly by the Senior Manager

Date of incident	Name of individual(s) involved	Device and location	Details of incident	Actions and reasons	Confirmed By