E-safety Policy

Table of Contents

Why E-safety?

The internet has changed considerably in the last years. Access to it by ever younger children is an increasing concern for parents, carers and practitioners. *"An increase in screen time has also resulted in a significant upward trend in online abuse." Ofcom, December 2020*

Technology has developed over recent years and will continue to evolve; children will often be the first to embrace new technologies. Technology has had, and will continue to have, a profound effect on the way we communicate. For example, texting, instant messaging online chat and emailing are for many a normal and accepted means of 'written' and spoken communication. Many young children learn to communicate through technology before they learn to read and write. It is important then to know how to safeguard children from dangers such as obscenity, malwares, scams, phishing, identify theft, cyberbullying, sexual exploitation, radicalisation etc. For more information including **parents' resources please see: Keeping children safe online | NSPCC**

The breadth of issues classified within online safety is considerable, but can be categorized into three 'C' areas of risk:

- *Content*: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
- *Contact*: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- *Conduct*: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

We refer to 'Safeguarding children and protecting professionals in early years settings: online safety considerations' to support this policy.

We provide training for staff in online safety and understanding how to keep children safe online via NDNA (https://moodle.ndna.org.uk) as part of their Induction training. If any concerns arise relating to online safety, then we will follow our safeguarding policy and report all online safety concerns to the DSL.

The DSL will make sure that:

- All staff know how to report a problem and when to escalate a concern, including the process for external referral
- All concerns are logged, assessed and actioned in accordance with the nursery's safeguarding procedures
- Parents are supported to develop their knowledge of online safety issues concerning their children via the Parents' Portal.

DSLs:
Miss Ingrid at Chelsea Pre-Prep, Miss Yria at Kingsland Pre-Prep and Miss Nicole at Grand West Pre-Prep. Miss Charly at Archmore Gardens Pre-Prep, Miss Lauren, assistant DoE, oversees and supports our DSLs.

Everyday E-safety procedures at our Pre-Preps

General steps we follow at Rocket Productions,

- ensuring that we have appropriate antivirus and anti-spyware software on all devices and update them regularly (this is managed by Abbey Systems)
- Ensure content blockers and filters are on all our devices, e.g. computers, laptops, tablets and firewalls to avoid access to inappropriate online content inside our schools
- Ensuring all devices are password protected. Passwords should be kept safe and secure, changed regularly and not written down
- Providing secure storage, work email and secure internal comms via Microsoft 365 Business Education plan
- Ensuring no personal social media or messaging apps are installed on Rocket Productions devices
- Reviewing all apps or games downloaded to ensure they are age and content appropriate and to enhance the current learning. Any apps must be approved first by the Head.

- Using only Rocket Productions devices to record/photograph children in the setting (e.g. to record their learning journey)
- No personal mobile phones are allowed to be used around children. Staff must lock their personal devices away on arrival and parents and visitors are asked not to use them when visiting or during drop-off/pick-up times
- Not permitting staff or visitors to access the Pre-Prep's Wi-Fi (all Pre-Preps have a guest service)
- Never emailing personal or financial information
- Ensuring all electronic communications between staff and parents is professional and takes place via our official communication channels, e.g. each staff member has a work email address or parents can call the Office. This is to protect staff, children and parents
- Staff understand that no one, either at work or in any other place, may deliberately download, possess, or distribute material they know to be illegal
- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Teaching children how to stay safe online and report any concerns they have (resources on https://www.nspcc.org.uk/keeping-children-safe/online-safety/)
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not; comparing people in real life situations to online 'friends'
- Providing parents with information on how to keep children safe online (see parents' portal and https://www.nspcc.org.uk/keeping-children-safe/online-safety/)
- Ensuring children are supervised if they have to use internet connected devices for teaching purposes

We are aware that Cyber criminals will target any type of business including childcare and hence we ensure all staff are aware of the value of the data and information we hold in terms of criminal activity in line with the Data Protection Act, e.g. scam emails. All staff are reminded to follow all the procedures within this E-safety policy, including backing up sensitive data in our cloud rather than devices, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the Head Teacher or DSL as soon as possible and these will be reported through the NCSC Suspicious Email Reporting Service at report@phishing.gov.uk

Internal work email, Microsoft Teams, SharePoint and OneDrive, computers and ipads and any other ICT resources must be used safely and only for work related purposes and in accordance with this E-safety policy. This policy also regulates the use of internet access, social networking and prohibits

the use of personal phones and smart devices during contact hours with children as well as personal cameras to photograph or record children.

Smart devices (e.g., mobile phones) and recordings

We take steps to ensure children are not photographed or filmed on video for any other purpose than to record their learning and development on Seesaw (online learning journal/portfolio) or their participation in events organised by us. Photographs and videos will not be taken in areas where intimate care routines are carried out.

Parents and visitors - We ask parents and visitors not to use their mobiles or camera devices whilst at the Pre-Prep to ensure the safety and privacy of our children. Parents may be allowed to take photos in their child's classroom, i.e. when coming to help with their child's class activities and when consent has been given by the other parents.

Parents sign a consent form before joining the Pre-Preps to allow us to take photographs/videos and to share these in displays and weekly information shared with their child's class and also for children's photos/videos/records to be uploaded to Famly. They also sign a consent form if they want to allow the use of digital images on our social media platforms and websites. Photographs or recordings of children are only taken on equipment belonging to the Pre-Prep or Rocket Productions and stored safely in the Pre-Prep's Microsoft 365 Education storage system. These will be deleted after each academic year and from the ipads on a daily basis and stored safely on SharePoint (Microsoft 365 Education storage system) on the class online folder.

Staff - We take steps to ensure that there are effective procedures in place to protect children, young people, and vulnerable adults from the unacceptable use of mobile phones, cameras and electronic devices with recoding and sharing capabilities in the setting.

Rocket Productions and Pre-Preps' devices will not be used for personal purposes such as social networking. Although we follow a hands-on project-based and play-based approach, we understand that the use of electronic toys, Computers, school iPads, school smart phones and Internet access in the classroom has its place. Digital literature is important for children as part of their educational journey, however this will always be planned to enrich and extend learning activities and filtered appropriate to the age of the children and the curriculum. Due to the young age of our pupils, any internet access will be supervised by a teacher.

Personal mobile phones belonging to members of staff are not to be used on premises during teaching hours and never when in direct contact with children. Staff phones must be kept in the lockers and only used during non-teaching hours (e.g. breaks) in the designated staff areas. If you are expecting a call, please provide your school Office number as your mobile needs to stay in the locker during 'working with children hours'. Any other personal smart devices and any other

electronic devices with imaging and sharing capabilities must not be used whilst working with children.

Staff will not use their personal mobile phones or any other personal recording devices to take photographs of children, we have a school phone or they can use their school Ipads.

Smart watches must be worn in 'flight or airplane mode' or with their Bluetooth disconnected, this will ensure there is no internet connectivity to access notifications or Wi-Fi. Staff understand they may not use their watch to receive calls or check messages whilst as this creates distraction and potential dangers.

If school iPads are taken home, they must be password protected and staff must always log off any school accounts accessed online (e.g. seesaw, outlook web...). remember to delete all photos of children therefore uploading any important/ needed photos to SharePoint. If leaving your iPad at school, please also remember to lock it away safely in a safe place or locker.

When using Famly both parents and teachers agree to keep their log in details safe and to not share these with anyone else. Teachers always log in and out safely from Famly after they finish working on it and all ipads are pin protected. Teachers are careful when tagging records on Famly and when posting comments. Any sensitive data or information must not be shared via Famly, instead please organise a meeting or call with parents.

Outings - A senior members of staff might be allowed to take their own mobile phone on outings for use in the case of an emergency however these will not be used for personal purposes and never to take photographs or record children.

Safeguarding is everyone's responsibility; therefore we expect staff to report anyone who is on breach our E-safety policy and/or misusing devices, internet or personal data including photographs and videos.

Staff use of Internet and Social Media

All members of staff are expected to adhere to this policy and ensure they know how to keep themselves and children safe online. Staff signs an e-safety/GDPR/privacy acknowledgement form when joining Rocket Productions.

Internet access must be used safely and only for work related purposes and in accordance with our E-safety policy. Each employee has a responsibility to report any misuse of the internet or email. By not reporting such knowledge, the employee will be considered to be collaborating in the misuse. Each employee can be assured of confidentiality when reporting misuse. Staff understand that no

one, either at work or in any other place, may deliberately download, possess, or distribute material they know to be illegal.

Staff should be aware that there are a number of legal implications associated with the inappropriate use of social media. Liability can arise under the laws of:

- Defamation
- Copyright
- Discrimination
- Contract
- Human Rights
- Protection from harassment
- Criminal Justice
- Data Protection

Staff must manage the settings of any social networking sites they pertain to in order to ensure their profiles and what they share are private. In addition, staff are required to establish professional boundaries when forming relationships with parents which includes not sharing information through social networking such as becoming friends with parents from their class or any of the Pre-Preps in sites such as Facebook or Instagram. We ask parents to respect our staff online privacy.

Staff are asked not to share any confidential data from to the Pre-Preps, Rocket Productions, children and families or anyone related to the company through any online forms.

Email and school communications

For any questions or issues, we ask parents and carers to strictly deal with the teachers and the Head as it would be unfair to discuss or spread confidential or inaccurate information via WhatsApp groups, emails, etc. Our Pre-Preps will be always willing to help with any questions or issues.

Parents have access to confidential information such as policies and procedures, important dates and events, photos, etc. This information must not be shared with anyone outside of Rocket Productions.

Staff at Rocket Productions use email as a means of communication with parents, i.e., class news, school's events, parents' partnership, etc. Emails can often contain photos of the children and information about our setting day-to-day operation that we consider parents should not share to other parties. Although prior joining our setting parents can choose to give consent to share class photos and contact details among the parents in their child's class, we do ask parents to never *forward* any school's email to avoid infringing our data protection and confidentiality policy and UK GDPR.

In addition, teachers will only use their work email account and will always *BCC* all parents/recipients when emailing more than 1 person in their emails. Emails containing sensitive information will be safely deleted as appropriate (Refer to GDPR Policy). Our email hosting software complies with the latest GDPR to ensure information is sent confidentially. Please notice is our pre-preps policy to only use **Microsoft OUTLOOK to manage your emails**, please do not add your account to your mobile or iPad mailbox, access them via Outlook instead and do not install any personal email accounts onto your work devices. This is so we can manage any lost devices or lose of data remotely if needed. We have a 2-factor authorisation system and use the 'authenticator app' to log in any of our Microsoft 365 accounts and apps.

Any use of our electronic communication systems (including email, internet and telephones) for purposes other than the duties of staff employment is not permitted. We expect all staff to use their common sense and good business practice when using email.

Emails must not be used to send abusive, offensive, sexist, racist, disability-biased, sexual orientation based or defamatory material, including jokes, pictures or comments which are potentially offensive. Such use may constitute harassment and/or discrimination and may lead to disciplinary action up to and including summary dismissal. If you receive unwanted messages of this nature, you should bring this to the attention of your Head Teacher.

Online Safety as part of Early Years Education

NCPCC Campaign

In early years education, it's essential to introduce children to the concepts of internet safety and digital citizenship at an age-appropriate level. At Rocket we celebrate Internet Safer Day bit also use the NCPCC campaign which we share with parents.
Meet Techosaurus, our new online safety dinosaur!

Children are growing up in a time where screens are everywhere and the internet plays a big part in their lives, even from a very young age.

This can be beneficial, they can learn new things, connect with friends and family, and have fun. But it's important to have conversations on how to explore the online world safely.

That's where **Techosaurus,** our new friendly dinosaur comes in!

We understand that talking about online safety can seem daunting, but it doesn't have to be. We have created **Techosaurus s**pecifically to make these conversations as easy as possible for you and your child.

Techosaurus is aimed at little ones who are starting to use technology and the internet, and keeps the conversation around online safety positive. **Techosaurus** will help your child to form healthy online habits, routines and behaviours from a young age, and build basic knowledge and skills related to online safety.

Play, Protect, Ask, Say

We want to make talking about online safety easy for you and your child, because we know that talking regularly with children about these important safety messages can make a big difference.

To help you get the conversation started, Techosaurus introduces **4 key messages** to share with your child. Each one offers simple, practical advice that can help keep your child safe online.

Play

Play and be kind online

The internet can be a lot of fun, and Techosaurus often finds lots of games to enjoy. But it's important to be kind while you're playing, letting everyone else have fun too!

Protect

Protect your personal information

Lots of important information can get shared online, such as your date of birth and address.

It's important to keep this information private and only share it with a safe adult you trust.

Ask

Ask before you try something new online

Always ask for advice from an adult you trust before you try something new online, it's much safer and more fun to learn together!

Say

Say if anything has made you feel upset

It's always good to talk to a safe adult you trust about anything that makes you feel sad, worried, or confused. It doesn't have to be a family member, it can be a teacher, a friend's parent, or any adult that you trust and feel safe around.

Whatever has happened, it's not your fault, and you will never get into trouble for speaking out.

Children and technology: Age-appropriate usage advice | NSPCC

Help keep children safe online with Techosaurus! | NSPCC

Resources for 3-11s - UK Safer Internet Centre

Legal Framework

- Working Together to Safeguard Children (2024) HMG
- What to do if you're worried a child is being abused (2015) HMG
- Early Year Foundation Stage (2024) DfE
- Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers (2024) HMG
- Keeping Children Safe in Education (2024) DfE
- Domestic Violence Risk Identification Matrix (2013) Barnardo's
- 'Safeguarding children and protecting professionals in early years settings: online safety considerations' (2019)

Safeguarding is a much wider subject than the elements covered within this single policy, therefore this document should be used in conjunction with our other policies and procedures.

Complaint Procedure

Stage 1

If any parent feels unhappy about any aspect of their child's care within the Pre-Prep they are advised to firstly speak to their child's keyperson (class teacher).

Stage 2

If the issue remains unresolved or parents feel they have received an unsatisfactory outcome, the teacher will report the issue to the Head Teacher who will then deal with the matter. The matter of concern must be raised within 3 working days if it relates to a particular incident. A written record will be securely and confidentially kept of any complaints (Complaints book). We hope that the issue will be dealt with satisfactorily by the Head Teacher. Depending on the matter parents will be notified within 28 days of the outcome of an investigation and action taken as a result of a complaint. Confidentiality will be maintained at all times, and data protection rules (see our Privacy Notice and GDPR Policy at the Parents Portal) will be observed when disclosing information to third parties.
Parents are always welcome to bring any matters straight to the attention of the Head Teacher if they so wish. Complaints and actions taken will be confidentially documented in our Complaints book stored in the Office.

Stage 3

If the matter is still not resolved, the Pre-Prep will hold a formal meeting between the Head Teacher, Stuart Bamford (CEO) and a member of the senior management team. This is to ensure that the matter is dealt with comprehensively. Alternatively, an independent hearing panel can be set up. The Pre-Prep will make a record of the meeting and document any actions. All parties present at the meeting will review the accuracy of the record and be asked to sign in agreement, a copy will be provided. This will signify the conclusion of the procedure.

Stage 4

If the matter cannot be resolved to their satisfaction, then parents have the right to raise the matter with Ofsted. Parents are made aware that they can contact Ofsted at any time they have a concern, including at all stages of the complaints procedure. Ofsted is the registering authority for nurseries in England and investigates all complaints that suggest a provider may not be meeting the requirements of their nursery's registration.

A record of complaints will be kept in our school (Complaints book). The record will include the name of the complainant, the nature of the complaint, date and time complaint received, action(s) taken, result of any investigations and any information given to the complainant including a dated response.
Parents will be able to access this record if they wish; however, all personal details relating to any complaint will be stored confidentially and will be only accessible by the parties involved. Ofsted inspectors will have access to this record at any time during visits and inspections to ensure actions have been met appropriately. Written records of complaints, including complaints resolved at the preliminary stage must be kept for a period of 3 years. Records will be kept confidential in line with the GPDR, except where a body conducting an inspection under section 163 of the Education Act 2002, or the Secretary of State, requests access to the records or other documents involved in the complaint.

Contact details for Ofsted:	By post:
Email: enquiries@ofsted.gov.uk	Ofsted
Telephone: 0300 123 1231	Piccadilly Gate, Store Street, Manchester, M1 2WD

Parents will also be informed if we are aware that Ofsted will be inspecting us and after inspection, we will provide a copy of the report to parents and/or carers of children attending the Pre-Prep. We will provide Ofsted on request with a written record of all complaints made within any specified period and the action which was taken as a result of each complaint.

The above procedures must be followed. OFSTED might not respond if these steps have not been followed and might refer you back to the Pre-Prep procedure for complaints.