Clowns Nursery Manor House Pre-School

Online Safety Policy

Clowns Nursery is committed to safeguarding and promoting the welfare of children and young people and expects *all* staff and volunteers to share this commitment.

Online Safety encompasses not only the internet but also wireless communications including mobile phones, android tablets, PC tablets, iPads, cameras, webcams, eBooks and smart watches and smart toys. Online safety also includes the consideration of media applications and a user's access to content and contact with others such as chat rooms, blogs, social networking sites, instant messaging, gaming and video broadcasting.

Safeguarding is everybody's responsibility and therefore an agreed, shared approach must be promoted by all staff, parents and children.

The influence and value of Information and Communication Technology (ICT) should be firmly embedded within the EYFS, and it must therefore be reflected in practice. The following policy is in place to protect children and staff to promote safe practices, minimise and inform regarding related risk and help encourage and modify behaviours related to access and use of online technologies.

Anti-cyberbullying

Online Safety, including cyberbullying, is explicitly taught in the rising 3 and rising 4 rooms using Childnet's Smartie the Penguin story. Internet Safety Day is celebrated each year across Clowns where children participate in age-appropriate activities. We are aware that cases of peer-on-peer cyber-bullying amongst nursery aged children is extremely rare, however we acknowledge that we must prepare and equip our pupils with strategies that they can use to keep themselves and others safe when they are online.

Strategies for teaching about cyberbullying include encouraging parents/responsible adults and staff to engage in conversations with children about the games and websites the children access, teaching children to be kind online by following our Golden Rules, not retaliating, and by teaching the children how to report cyberbullying if it happens to them or someone else.

Cyberbullying involving parents/carers and staff members.

Parents are required to treat all Clowns employees, regardless of their position in the nursery, with respect, both in person and online. Incidents of cyberbullying involving parents/carers and staff should be reported to the Online Safety Officer, the Manager and the deputy manager who will follow appropriate procedures to support the staff member and resolve the issue(s).

Staff are required to conduct themselves appropriately online and they should follow Staff Behaviour Policy when engaging with social media. Staff are required to adhere to the Social Media Policy as detailed in the Staff Handbook.

MANAGEMENT

We place great importance on having a clear and written Online Safety Policy, with the following aims:

- To protect all users of information and communication technologies from potential and known risks.
- To establish a culture which ensures the safety and well-being of children, this includes their online safety, and which also safeguards all staff members in encouraging them to work safely and responsibly and to monitor their own behaviours, standards and practice.
- To recognise that we cannot stop advances in technology, and nor should we try to do so. Developmentally

appropriate access to computers and the internet in the early years contributes significantly to children's enjoyment of learning and development. Locked down and banning practices do not provide effective safeguards as prohibiting access to online technology within early years settings gives a false sense of security. Children have rights as learners and should be entitled to have access to appropriate technologies. They need to be empowered with the knowledge and skills to keep safe online and our policy aims to promote awareness and provide information and support to parents/carers and staff. By encouraging a balanced use of ICT for all children within the home and nursery we believe this contributes to their learning and development.

- To open a dialogue with parents, staff and children to prevent any future exposures to risk.
- To comply with the law on child protection and safeguarding, discrimination, data protection and health and safety.
- To minimise the risk of a data breach.

The overall responsibility for Online Safety lies with the Designated Safeguarding Lead (DSL), although we have appointed an additional Online Safety Officer. The DSL and Online Safety Officer have responsibility for diligently ensuring online safety practice is managed and implemented effectively, within the requirements of the law, to include:

- Ensuring our ICT system's security and virus protection are reviewed and updated regularly, to include a secure, filtered, managed internet service and broadband provider.
- Completing a monthly online safety audit with the Assistant Operations Manager and Accounts Administrator.
- Ensuring that our IT company carries out an enhanced online safety audit of all appropriate technologies (laptops, PCs, tablets) at least three times in every academic year, towards the end of each term (end of November, April, July). Each time, a report with the findings and any recommendations will be produced and given to both the Manager and the Online Safety Officer. All recommendations are to be considered and, if appropriate/necessary, actioned within no longer than a month from the date of receipt of the report.
- Reporting any online safety incidents to CEOP (Child Exploitation and Online Protection) 0870 000 3344 and keeping a log.
- Embedding online safety during staff induction and arranging online safety training for staff with an outside provider (such as SWGfL - South West Grid for Learning Trust Ltd and a Primary Computing consultant of LGfl or National Online Safety) as and when deemed suitable.
    - All staff complete online safety training, via our Training Hub/Portal in the Autumn term, with refresher courses scheduled for the Spring and Summer Terms.
- The DSL, Online Safety Officer and Assistant Operations Manager complete an annual online training course with 'National Online Safety', to ensure they are up to date with the latest in Online Safety. They will also attend additional short courses from the NOS and outside agencies as required keeping up to date with changes and advances with regards to online technologies.
- Ensuring staff and parents receive relevant information about emerging issues. This will include updating the Online Safety Section of the website with age-appropriate online guides, relating to internet use and safety at home.

Data protection:

- Clowns Nursery Care Ltd are registered with the Information Commissioner's Office (ICO) under the GDPR

Data Protection Act of 2018. Our registration number is Z7395021, and this is renewed annually in April.

- Memory sticks are stored securely at all times, and where possible worn upon one's person (by badge/clip or necklace). The Online Safety Officer has password protected, encrypted USBs which the staff can obtain for the purposes of completing planning at home. The Online Safety Officer, Assistant Operations Manager or Accounts Administrator can request nursery USB sticks to be handed in at any time, for the purpose of checking the stored content. Permission for any other documents that may need to be saved to the USB will need to be requested and shown to the Online Safety Officer. Under no circumstance can photographs or details pertaining to any child be saved onto the USB device. The only exception is the Clowns event photo USB stick, which is encrypted and is never taken offsite. When children leave, their photos are deleted off the device in accordance with the Data Retention Policy.
- Memory cards from cameras are always stored securely. Cameras and keys to lockable cupboards in classrooms are signed out from Reception in the morning and signed back in at the end of the day. The upload of photographs from cameras is strictly controlled, with only team leaders/teachers or a designated member of staff in each room undertaking this task. Each time photographs are uploaded / printed off using the classroom computer, for any reason, the class must complete the appropriate form, detailing the activity.
- Photos of children are only used in the Learning Journals, subject or classroom displays within the password protected area of the Clowns website or on the online Learning Platform Seesaw, with the permission of parents.
- There are 3 designated laptops solely for the upload of photos, if required. Each classroom has an account and password on each laptop, within which they can upload their photos. All photographs are deleted from all accounts at the end of each academic year.
- Photos are not emailed to or from Clowns. Parents are regularly reminded that we do not print off or accept photographs of the children by email. Parents who email photographs in are sent a reminder by email that they are now required to bring in hard copies of any photographs they would like to share.
- All information other than that held on the computer is locked away in either cupboards or drawers and when no longer needed is shredded. No confidential material is ever removed from the nursery unless it is password encrypted and specifically authorised by Tracy Landy. Keys to these cupboards/drawers are held by Tracy Landy, the Deputy, the Third-in-Charge and the Operations Manager (Online Safety Officer).
- All computer equipment is password protected. Management have a central list of all login details. If a password is altered the Online Safety Officer *must* be informed as soon as possible.
- Our new online learning platform, Seesaw, is an extension of the classroom. We do not upload any personal information on Seesaw and the parents are only able to see information related to their child(ren). The parents have dedicated access and can choose how to share any information or pictures from home. The Designated Safeguarding Lead, Online Safety Officer, Assistant Operations Manager and Accounts Administrator have administration access on Seesaw and can see everything that has been uploaded. The class teachers and administrators with Class Teacher access need to approve any photographs or short videos that are uploaded by parents and class teachers. The platform can be accessed online but only by those with login permissions. Our Acceptable Use Agreement states that accessors agree not to disseminate any information to third parties to work in line with our Confidentiality and Sharing of Information Policy **(see 7.4**. **Confidentiality and Sharing of Information Policy and Procedure)**
- To enable classrooms to upload the children's work and photographs onto Seesaw, the classroom USB ports are unlocked between 10am and 5pm, Monday to Friday. Weekly checks will be carried out on the computers to ensure that no photographs are being stored on the classroom computers.
- Our First Steps software package is an online worked site and can be accessed outside the nursery but only

with authorisation from Tracy Landy and by those with login permissions. Our Acceptable Use Agreement states that accessors agree not to disseminate any information to third parties to work in line with our Confidentiality and Sharing of Information policy.

- The Online Safety Officer ensures that the Assistant Operations Manager and Accounts Administrator perform spot checks on internet history every month and will review the findings. All classroom computers have had the ability to erase history disabled. Regular checks are performed to ensure we are protected against unverified internet material being viewed in the classroom.
- Clowns Nursery has cyber and data liability cover with Towergate Insurance.

  This protects us from:

  - Denial of service attack. This is bombardment of the internet meaning we cannot get on to the internet.
  - Cyber business interruption
  - Data breach following loss of laptops or USB sticks
  - Data breach following hacking or employee theft. If compromised this would be a problem due to data protection issues and client confidentiality.

STAFF

All staff need to understand the significance of online safety, which highlights the importance of safeguarding children and keeping them safe, which is of paramount importance.

All staff receive ongoing appropriate training and guidance in order to effectively implement online safety. As part of induction, and renewed annually, every staff member is required to read, sign and agree to adhere to the updated AUA (Acceptable Use Agreement), which they must sign and return to the Online Safety Officer or Assistant Operations Manager. Staff are given an opportunity to openly discuss online safety in staff meetings and during supervision, as a part of child protection and safeguarding and can bringing up any online safety issues that they may have.

Clowns Nursery Senior Leadership Team also benefit from a nursery's membership to National Online Safety, which has courses that can be shared with the wider staffing team. All SLT members are required to join the National Online Safety Training and Learning Hub via the nursery's School Membership of National Online Safety. Each staff member has individual access to numerous resources and CPD certified training, accessible within their Learning Hub. A record of all training undertaken is accessible to the DSL, Online Safety Officer and Assistant Operations Manager.

Within the National Online Safety Platform, the DSL, Deputy Head and Online Safety Officer also set a timetable of training and webinars to be shared with staff, as and when required throughout the year.

As a part of the NOS membership the SLT will receive a monthly webinar link and newsletter in their personal email addresses, detailing the most recent advances or updates with regards to National Online Safety, keeping them informed and up to date. Thess are shared, in turn, with the wider staffing team. All resources can also be accessed via the free National Online Safety Mobile App, ensuring all staff members are able to access all training, at all times.

Staff are always expected to follow the guidelines below:

- IT equipment and smart devices belonging to Clowns should never be used to access inappropriate material, such as obscene, hateful, pornographic or otherwise illegal material.
- Personal equipment containing inappropriate material should not be brought into the nursery.

- Staff are aware of the risks of fostering online relationships with parents and children.
- Staff are aware of their responsibility of confidentiality, inside and outside working hours.
- Staff are aware of their digital footprint (a trail of data created whilst using the internet), and that the use of social networking sites (such as Facebook, Twitter, Instagram) in staff recreational time on their own devices must not compromise professional integrity or bring the nursery into disrepute.
- Staff are reminded that adding parents as 'friends' on social network sites or using their personal IT equipment, i.e., smart phone or tablet, to communicate with parents is not permitted under the nursery's Communications and Software Policy.
- Staff are made aware of the risk from computer viruses, opening and clicking on links within emails received from unknown sources which may contain potentially harmful malware.
- Staff must inform the Online Safety Officer or Assistant Operations Manager if they intend to change the login details on their classroom computer or other nursery software programs.
- **All nursery computers should always be locked when unattended.** This includes brief periods away from the computer, even when the room is empty. If there is no one physically *at* the computer, it should be locked.
- No child should ever be left unsupervised whilst using any IT equipment. We only use child moderated sites, and our secure filtered internet server is used to monitor and prevent offensive material or spam. If, on rare occasions, security systems are not able to identify and remove such materials, the material should be minimised from the desktop and the computer staffed whilst the incident is reported to the Online Safety Officer or Assistant Operations Manager immediately.
- Computers should be placed in areas of high visibility which will enable children and adults to be closely supervised and their online use to be appropriately monitored.
- The Health and Safety Officer distributes 'Display Screen Equipment' workstation checklists to all computer users to ensure the correct and safe use of computer equipment is applied.
- Although children should only be able to access age-appropriate websites, staff should encourage children and parents to be cautious about any information given to them by other users on such sites and must recognise that everyone may not be who they say they are i.e., Stranger Danger.
- Staff are required to sanitise the laptops after each use. Once sanitised the laptop must be closed, and the exterior wiped over. It is important to turn the computer off before sanitising.

PARENTS

We have developed an Acceptable Use Agreement (AUA) which details the ways in which the internet can and cannot be used in the nursery. We are responsible for the safety of children in our care but also for the behaviours and expectations of any adults who affect or come into contact with the early years setting. All staff must read and sign their agreement.

All parents are provided with a copy our Online Safety Policy upon joining the nursery. The policy is accessible to parents to ensure they have an awareness of our online safety procedures and can take a part in promoting online safety within the nursery, at home and in the community. Parents are made aware that they are able to view the full policy and Acceptable Use Agreement via the website.

It is essential for parents and carers to be fully involved with promoting online safety within the setting, home and social environment. It is therefore advantageous to consult and discuss emerging online safety issues with parents and carers. Our general information sheets that parents are required to complete prior to their child commencing at the nursery now include a section on their child's use of Information and Communication technologies. This information is then shared with the child's keyworkers encouraging a broader understanding of

the benefits and risks of ICT use. This information would also draw attention to the Online Safety Officer and Assistant Operations Manager for any areas of concern that may need to be reviewed within our policies.

Training sessions for staff on online safety are held at the nursery on an annual basis (usually in the Spring Term) and at any time deemed suitable to renew by management. All information our practitioners receive will be passed on to parents and carers through leaflets, booklets and recommended online safety books.

Since September 2021, the SLT have access to National Online Safety, including short courses and updates to national online safety policies, procedures, and practices – all of which can be shared with the wider staffing team.

Parents of children at the nursery also benefit from our membership to National Online Safety. All parents are invited to join the National Online Safety Parent Training and Learning Hub. Each family is a sent a link where they can create an account which gives them access to a Parent Online Safety course and numerous parent-specific printable guides, webinars and video resources appropriate to the age(s) of their child(ren). Parents can also choose to sign up to receive the regular online safety updates, if they would like to.

CHILDREN

Membership to National Online Safety also gives the Senior Leadership Team access to additional online resources which can be shared with teachers to further enhance their experience of teaching children about online safety. There are online guides, explainer videos and age-appropriate short video lessons and accompanying written lesson plans which are ready to use but can also be modified as required. The topics covered within Early Years are 'Health, Wellbeing and Lifestyle', 'Privacy and Security', 'Managing Online Information', 'Self Image and Identity', 'Online Relationships', 'Online Bullying, 'Online Reputation' and 'Copyright and Ownership'.

SANCTIONS

We will follow our disciplinary policy and procedure in line with our staff handbook for dealing with the inappropriate use of ICT both onsite and offsite (where known).

The Online Safety policy must operate in conjunction with other nursery policies including *Health and Safety, Safeguarding and Child Protection, Confidentiality and Sharing of Information, Computer Access, Photography Video and Imaging Policy, Mobile Phone Policy, Privacy Policy* and *Whistleblowing Policy*.

Reviewed August 2023