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.

We always consider the 4 Cs of Online Safety (Content, Contact, Conduct and Commerce) when implementing, reviewing and updating our Online Safety Policy. These four pillars underpin our commitment to promoting a safe digital environment for all staff, children and families at Clowns.

Online Safety encompasses not only the internet but also wireless communications including mobile phones, android tablets, PC tablets, iPads, cameras, webcams, eBooks, 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 everyone'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 to 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 stories, although he is a visible mascot in all rooms, where he can be seen near the main classroom computers. 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 Head and the Deputy Head 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 the Staff Behaviour Policy (**19.7**) 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 Leads (DSLs),** although we have appointed additional Online Safety Officers. The DSL and Online Safety Officers have responsibility for diligently ensuring online safety practice is managed and implemented effectively, within the requirements of the law, to include, but not limited to:

- 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 Front Office Manager and Accounts Administrator.
- Ensuring that our IT support company carries out a Vulnerability Scan on both our network and website every 3 months (March, June, September, December). Each time, a report with the findings and any recommendations is to be produced and provided to the nursery. The DSL and Online Safety Officers will consider all recommendations and, if appropriate/necessary, action them within one month from the date of receipt of the report.
- Ensuring an enhanced online safety and general computer audit of all appropriate technologies (laptops) at the end of every academic year (July / August). The accounts on each laptop will be checked by our IT support company and laptops 'cleaned' in time for the new academic year. As all documents are stored on our secure server, any documents found on the laptops will be deleted in preparation for the upcoming academic year. The IT support company will communicate with the Online Safety Officer regarding any upgrades and repairs required.
- Any electronic devices (laptop / tablet / computer) that are no longer in good working condition will be securely disposed of and/or destroyed by our IT support company in line with current data protection rules and regulations.
- Each time, a report with the findings and any recommendations will be produced and given to both the Head 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. The Front Office Manager and Online Safety Officer will be required to liaise with our IT company and to ensure appropriate recommendations are actioned in a timely manner.
- 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 - Southwest Grid for Learning Trust Ltd and a Primary Computing consultant of LGfl or NDNA) as and when deemed suitable.

- All staff complete online safety training during the Spring Term. They can also complete refresher training via our Training Hub/Portal in the Summer and/or Autumn Terms.
- The DSLs, Online Safety Officer and Front Office Manager complete an annual online training course to ensure they are up to date with the latest in Online Safety. They will also complete additional short courses on our training hub and/or via outside agencies as required in order to keep 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.

Network Content Filtering:
Our nursery internet network has strict content filtering, in line with working with a vulnerable age group (under 5s). This applies to all computers and IT devices that are connected to our network, without exception. The list of content to be filtered is not exhaustive and includes:

- pornography
- child exploitation and sexual content
- foul language and swearing
- all explicit and/or graphic imagery
- weaponry
- drug use

As there is often a need to access additional websites we have 2 filter levels within the nursery, both of which remain within the strict content filtering.

- Filter Level 1: All computers and laptops throughout the nursery, unless specified otherwise.
- Filter Level 2: Computers with additional access for the purpose of being able to fully carry out their administrative roles, in line with their job descriptions and level of responsibility within the nursery.

Filter Level 2 (all Filter Level 1 restrictions apply with the exception of Twitter, Facebook, LinkedIn, Instagram) is applied to the following computers in order to allow Safer Recruitment, Safeguarding and Additional research relating directly to the management, implementation and update of current policies, procedures and curriculum practices.
The computers with Filter Level 2 are used solely by the Head, Deputy Head, Operations Manager, and Development Manager. They have access to an additional hot desk computer in the upstairs office which has Filter Level 2.

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) to minimise the chance of these being lost or misplaced. The Online Safety Officer has password protected, encrypted USBs which the staff can obtain for the purposes of completing planning at home. The Head, Deputy Head, Online Safety Officer, Front Office 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 solely restricted to Monday to Friday,7.30am - 6pm, when the class USB ports are accessible.

- Photos of children are only used in nursery or classroom displays or Learning Journals, with the permission of parents.
- There are designated laptops which staff can use 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 can send in a hard copy of any photographs or upload them onto their child's Online Learning Journal.
- 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 The Head. Keys to these cupboards/drawers are held by the Head, the Deputy Head, a member of the Senior Leadership Team 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 Online Learning Journal is an extension of the classroom. We do not upload any personal information onto the Online Learning Journal and the parents are only able to see information related to their child(ren). The parents have dedicated access and can choose to share any information or pictures from home. The Designated Safeguarding Leads, Online Safety Officers, and Administration Team have administration access on the Online Learning Journal and can see everything that is uploaded.

Each room has designated team members, e.g. Class Teachers and Team Leaders, who need to approve any observations, photographs or short videos that are uploaded by parents or staff members – before they can be added to the child's Learning Journal. The Online Learning Journal 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 and Procedure **(see 7.4)**

- To enable classrooms to upload the children's work and photographs onto our Online Learning Journal platform the classroom USB ports are unlocked between 7.30am and 6pm, Monday to Friday only. The USB ports for the Head, Deputy Head, Operations Manager and Development Manager's computers are unlocked between 7.30am and 7pm Monday to Friday only. The extended timeline is to allow for the additional hours that are often worked by these staff members. Regular checks will be carried out on the computers to ensure that no photographs are being stored on the classroom computers.
- Our Nursery Management software package is an online worked site and can be accessed outside the nursery but only with authorisation from The Head 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 Accounts Administrator or Front Office Manager performs 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.
- Ensuring an enhanced online safety and general computer audit of all appropriate technologies (laptops) at the end of every academic year (July / August). The accounts on each laptop will be checked by our IT support company and laptops 'cleaned' in time for the new academic year. As all documents are stored in our secure server, any documents found on the laptops will be deleted in preparation for the upcoming academic year. Our IT support company will communicate with the Online Safety Officer regarding any upgrades and repairs required.
- Any electronic devices (laptop / tablet / computer) that are no longer in good working condition will be securely disposed of and/or destroyed by our IT support company in line with current data protection rules and regulations.
- 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, especially its connection to 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 Front Office 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.

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 Front Office 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. All computers have a 10-minute lockout policy applied to them. This means that they automatically lock the screen if there has been no activity for 10 minutes.
- 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 Front Office 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 Head of Pastoral, who leads on Health and Safety, 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 our 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 via the Documents section in our Online Learning Journal to ensure they have an awareness of our online safety procedures and can take 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 and within the documents section of our Online Learning Journal.

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 Front Office 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 the management team. All information our practitioners receive will be passed on to parents and carers through leaflets, booklets and recommended online safety books.

CHILDREN

Smartie the Penguin is our online safety mascot and helps reinforce the understanding that, before going online, the children need to ask an adult.

Smartie the Penguin is a series of 6 stories created, by www.childnet.com, for 3 to 7 year olds to help them to explore life online and understand how and when to ask for help. The first two stories in the series are specifically for the EYFS and cover the following themes:

- Story A: Seeing upsetting content, unreliable information, and being asked for personal information
- Story B: Adverts, searching online, and online bullying.

In each story Smartie the Penguin encounters three different scenarios. Each time, the children are encouraged to talk about what has happened and explain what they think Smartie should do and why. In every story, the children are also asked to join in with Smartie's special song, to help him make his decisions!

SCHOOL PROVIDED MOBILE DEVICES

Each classroom is provided with up to 4 tablets to enhance teaching and learning and these should be used appropriately. The tablets are Wi-Fi only and subject to the same restrictions and filters as the classroom computers.

Staff must ensure that any image or sound recordings made on the devices are in line with the parental consent forms and permissions are as per each child's record.

Use of Tablets:
The tablets are managed centrally which enables the nursery to monitor their use, as well as to manage the apps that are installed on them.

- Apps:
  - The staff and children regularly use apps to enhance teaching and learning in the classroom.
  - In order to have an app installed a request is made to the Online Safety Officer who checks the app to ensure age appropriateness and suitability. Once approved the app is downloaded to devices by the Front Office Manager, and this update will be applied to the tablets.
  - The Front Office Manager is required to keep a list of accessible apps.
- Taking images and video:
  - Tablets are used in line with the school's Photography, Imaging and Video Policy (**see 7.3**).
- Internet Access:
  - The tablets have internet access so that staff may upload videos and images to children's online learning journals. Any access is limited by the filtering system so that children and staff cannot access inappropriate websites.
- Lost or stolen equipment:
  - All school devices are asset logged. Serial numbers are logged along with the rooms the devices are allocated to.
  - The Online Safety Officer has the ability to clear or lock a device remotely if needed.
  - The devices are also protected using Smartwater, which is a traceable liquid and forensic asset marking system (taggant), applied to items of value to identify thieves, and deter theft.

SANCTIONS

In the event of any breach of expectations in relation to ICT 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(8.1.1); Safeguarding and Child Protection (6.1.1); Confidentiality and Sharing of Information(7.4); Computer Access (7.1.3); Photography Video and Imaging Policy (7.3); Mobile Phone, Electronic Device and Wearable Technology Policy (7.2); Privacy Policy (7.5)* and *Whistleblowing Policy (5.3)*.

Reviewed 27th August 2025