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.

This policy applies to _all_ staff, including senior staff managers, paid staff, volunteers, agency staff, students or anyone working on behalf of Clowns Nursery.

Online Safety (also referred to as e-safety) encompasses not only the internet but also wireless communications including mobile phones, cameras, webcams, iPads, ebooks and PC tablets. 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 ICT should be firmly embedded within the EYFS and it must therefore be reflected in practice. The following policy is in place to help modify behaviour and to promote acceptable use of online technologies.

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 discrimination, data protection and health and safety.

- To minimise the risk of a data breach.

We have an appointed Online Safety Officer, who has overall responsibility for 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.

- Ensuring that our IT company carries out an enhanced online safety audit of all appropriate technologies (laptops, PCs, tablets) twice in every academic year, once during February and again at the beginning of

- August. Both times, a report with the findings and any recommendations will be produced and given to both the Manager and the Internet 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 (SWGfL - South West Grid for Learning Trust Ltd and a Primary Computing consultant of LGfl) as and when deemed suitable.

- The Online Safety Lead completes an annual online training course (with High Speed Training) to ensure they are up to date with the latest in Online Safety.

- Ensuring staff and parents receive relevant information about emerging issues.

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. Any documents that need to be saved to the USB will be sent to the Online Safety Officer or Administration Assistant who will upload the document onto the USB for the member of staff.

- 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. There are 3 designated laptops solely for the upload of photos. Each classroom has an account and password on each laptop, within which they can upload their photos. Photos of children are only used in the Learning Journals, subject or classroom displays or within the password protected area of the Clowns website, with the permission of parents.

- 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 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 Operations Manager/Online Safety Officer and Accounts Administrator perform spot checks on internet history every month. 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 have received appropriate training and guidance in order to effectively implement online safety. As part of their induction, each staff member is given a copy of our Online Safety policy, procedures and an AUA (Acceptable Use Agreement), which they must sign and return. Staff are given an opportunity to openly discuss online safety in staff meetings and during supervision.

Staff are always expected to follow the guidelines below [DEL at all times]:

- IT equipment 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 in to 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 against nursery policy.

- Staff are made aware of the risk from computer viruses, and opening emails from unknown sources.

- Staff must inform the Online Safety Officer if they intend to change their login details.

- **Any accessible computer 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 ICT 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 manned whilst the incident is reported to the Online Safety Officer 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 has distributed 'Display Screen Equipment' workstation checklist 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.

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 summary of our online safety policy upon enrolment at the nursery, 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 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 at times when 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.

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, Camera and Image Policy, Mobile Phone Policy, Privacy Policy and Whistleblowing.