Squirrel Lodge Nursery



Online Safety Policy incorporating:

* Acceptable Use of Technology.

**Written and adopted: March 2021**

Claire Elliott-Hare has overall responsibility for the implementation of this policy. It will be reviewed at least annually.

Reviewed: March 2022

Reviewed: March 2023

Reviewed: January 2024

Reviewed: February 2025

Next review date: February 2026

**Key contact personnel**

Claire Elliott-Hare has overall responsibility for child protection across the organisation. She is a Designated Safeguarding Lead along with Terrie Platt, Manager. The Deputy Designated Safeguarding Lead is Ester Rowe.

**Key Contacts**

|  |  |  |
| --- | --- | --- |
|  | **Name** | **Contact information** |
| **Designated Safeguarding Lead (DSL)** | Claire Elliott-Hare | [squirrellodgenursery@hotmail.com](mailto:squirrellodgenursery@hotmail.com)  07842441237 |
| **Designated Safeguarding Lead (DSL)** | Terrie Platt, Manager | [squirrellodgenursery@hotmail.com](mailto:squirrellodgenursery@hotmail.com)  07842441237 |
| **Proprietor, Registered person** | Claire Elliott-Hare | [squirrellodgenursery@hotmail.com](mailto:squirrellodgenursery@hotmail.com)  07842441237 |
| **Designated Safeguarding Lead Deputies** | Ester Rowe, Senior Practitioner | [squirrellodgenursery@hotmail.com](mailto:squirrellodgenursery@hotmail.com)  07842441237 |

**This is a core policy that forms part of the induction for all staff. It is a requirement that all members of staff have access to this policy and sign to say they have read and understood its contents**.

1. **Policy Aims**

* This policy has been written by Squirrel Lodge Nursery, building on the Kent County Council/The Education People policy template, with specialist advice and input as required.
* It takes into account the DfE statutory guidance ‘[Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)’ 2023, [Early Years and Foundation Stage](https://www.gov.uk/government/publications/early-years-foundation-stage-framework--2) 2024 ‘[Working Together to Safeguard Children](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2)’ 2023 and the [Kent Safeguarding Children Multi-Agency Partnership](http://www.kscb.org.uk) procedures.
* The purpose of our online safety policy is to:
  + Safeguard and protect all staff members, children, parents/carers and service users.
  + Identify approaches to educate and raise awareness of online safety throughout our settings.
  + Highlight our acceptable use of mobile, smart technology and social media.
  + Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  + Identify clear procedures to use when responding to online safety concerns.
* Squirrel Lodge Nursery classifies the issues and risks with smart technology and online safety into four areas of risk:
  + **Content:** being exposed to illegal, inappropriate or harmful material
  + **Contact:** being subjected to harmful online interaction with other users
  + **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
  + **Commerce:** risk of financial harm and cyber-crime

1. **Policy Scope**

* We believe that managing smart technology, images and online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
* We identify that the internet and associated devices, such as computers, tablets, mobile phones, smart watches, games consoles, and other smart and electronic devices, are an important part of everyday life.
* We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risks online.
* This policy applies to all staff including the management team, staff, external contractors, visitors, families, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as children, parents and carers.
* This policy applies to all who access to the internet and use of smart technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones, etc.

**2.1 Links with other policies and practices**

This policy links with several other policies, practices and action plans including:

* Anti-bullying policy
* Behaviour Management policy
* Child Protection policy
* Confidentiality policy
* Employee Handbook
* Code of Conduct
* GDPR policy
* Managing Allegations Against Staff and Volunteers policy
* Parental Responsibility policy
* Use of Cameras and Images policy
* Acceptable use of technology

1. **Monitoring and Review**

* Technology in this area evolves and changes rapidly. We will review this policy at least annually.
  + The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
* We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
* To ensure Squirrel Lodge Nursery has oversight of the use of smart technology, images and online safety, the DSL will be informed of any concerns, as appropriate.
* Any issues identified via monitoring will be incorporated into our action planning.

1. **Roles and Responsibilities**

* The Designated Safeguarding Leads (DSL) have lead responsibility for implementing the online safety within the setting.
* We recognise that all members of staff have an important role and responsibility to play with regards to ensuring this policy is adhered to.

**4.1 The management team will:**

* Ensure that smart technology used meets the safety IT requirements and that the usage meets the requirements of this policy.
* Ensure that any images taken and used meet the requirements and processes of this policy.
* Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
* Ensure there are appropriate and up-to-date procedures in place to manage all aspects of this policy.
* Ensure that suitable and appropriate filtering and monitoring systems are in place
* Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
* Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
* Ensure there are robust reporting channels for staff to access regarding online safety concerns, including internal, local and national support.
* Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
* Audit and evaluate online safety practice to identify strengths and areas for improvement.

**4.2 The Designated Safeguarding Lead (DSL) will:**

* Act as a named point of contact on all technology safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
* Work alongside deputy DSLs to ensure the use of smart technology, images, and online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
* Ensure all members of staff receive regular, up-to-date and appropriate training.
* Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
* Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with staff and families, as appropriate.
* Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
* Ensure that the use of smart technology, images and online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
* Maintain records of concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
* Monitor incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
* Report concerns, as appropriate, to the owner.
* Work with the management team to review and update policies on a regular basis (at least annually).

**4.3 It is the responsibility of all members of staff to:**

* Contribute to the development of this policy.
* Read and adhere to the policy and other relevant policies.
* Take responsibility for the security of setting systems and the data they use or have access to.
* Model good practice when using technology and maintain a professional level of conduct in their personal use of smart technology, both on and off site.
* Embed online safety education in curriculum delivery, wherever possible.
* Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
* Identify concerns and take appropriate action by following the settings safeguarding policies and procedures.
* Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
* Take personal responsibility for professional development in this area.

**4.4 It is the responsibility of staff managing the technical environment to:**

* Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate policies and procedures.
* Implement appropriate security measures as directed by the DSL to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
* Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the staff team.
* Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the staff team
* Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

**4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:**

* Engage in age appropriate education opportunities under direct supervision from staff.

**4.6 It is the responsibility of parents and carers to:**

* Read the policies and encourage their children to adhere to the policy.
* Support our online safety approaches by discussing issues with their children and reinforcing appropriate and safe behaviours at home.
* Role model safe and appropriate use of technology and social media.
* Identify changes in behaviour that could indicate that their child is at risk of harm online.
* Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
* Use our systems, such as learning platforms, and other network resources, safely and appropriately.
* Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

1. **Education and Engagement Approaches**

**5.1 Education and engagement with learners**

* We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
  + Ensuring education regarding safe and responsible use precedes internet access.
  + Promote and include online safety in EYFS activities to support children’s learning and awareness.
  + Reinforcing online safety messages whenever technology or the internet is in use.
  + Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  + Key rules shared with children will be:
    - I only go online with a grown-up;
    - I am kind online;
    - I keep information about me safe online (if age appropriate);
    - I tell a grown-up if something online makes me unhappy or worried.
  + Parents will sign a declaration to confirm they accept our Technology AUP. Please see Appendix 1.
* We will support learners to understand the policies in a way which suits their age and ability by:
  + Informing staff, partners, visitors, children and their families that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  + Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  + Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

**5.2 Training and engagement with staff**

We will:

* Provide and discuss the acceptable use of smart technology, images and online safety policy and procedures with all members of staff as part of their induction.
* Provide up-to-date and appropriate training for all staff on a regular basis, with at least annual updates.
  + This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
* Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
* Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
* Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
* Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
* Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.
  1. **Awareness and engagement with parents and carers**
* We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
* We will build a partnership approach to online safety with parents and carers by:
  + Providing information and guidance on the online safety policy in a variety of formats.
  + Drawing their attention to the policy and expectations in newsletters, letters, our prospectus and on our website.
  + Requesting that they read key information as part of joining our setting.
  + Requiring them to read our policies and discuss the implications with their children.

1. **Reducing Online Risks**

* We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
* We will:
  + Regularly review the methods used to identify, assess and minimise online risks.
  + Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  + Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  + Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
* All members of staff are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

**7.Safer Use of Technology**

**7.1 Setting Use**

* We use a wide range of technology. This includes access to:
  + Laptops, phones
  + Tablets
  + Internet which may include search engines and educational websites
  + Emails
  + Digital cameras, etc.
* All devices will be used in accordance with our policies and with appropriate safety and security measures in place.
* No staff should access or use work related devices to send information to their personal devices.
* Members of staff will always evaluate websites, tools and apps fully before use in the setting or recommending for use at home.
* We will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the service/setting.
* We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
* Supervision of learners will be appropriate to their age and ability.
  + **Early Years Foundation Stage**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

**7.2 Managing Internet Access**

* All staff, learners and visitors will read our online safety policy before being given access to our computer system, IT resources or internet.

**7.3 Filtering and Monitoring**

**7.3.1 Decision Making**

* Senior management have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner’s exposure to online risks.
* We are aware of the need to prevent “over blocking”, as that may unreasonably restrict what can be taught and accessed, with regards to online activities and safeguarding.
* Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
* Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
* The management team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
* All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

**7.3.2 Filtering**

* Education broadband connectivity is provided through a reputable provider.
* The filtering system blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
* The filtering system blocks all sites on the [Internet Watch Foundation](https://www.iwf.org.uk/) (IWF) list.
* If anyone discovers unsuitable sites, they will be required to:
  + turn off monitor/screen and report the concern immediate to a member of staff.
  + The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
  + The breach will be recorded and escalated as appropriate.
  + Parents/carers will be informed of filtering breaches involving their child.
* Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

**7.3.4 Monitoring**

* We will appropriately monitor internet use on all owned or provided internet enabled devices.
* If a concern is identified via monitoring approaches we will:
  + Respond in line with the child protection policy.
* All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

**7.4 Managing Personal Data Online**

* Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
  + Full information can be found in our information GDPR policy.

**7.5 Security and Management of Information Systems**

* We take appropriate steps to ensure the security of our information systems, including:
  + Virus protection being updated regularly.
  + Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  + Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  + Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  + Regularly checking files held on our network,
  + The appropriate use of user logins and passwords to access our network.
  + All users are expected to log off or lock their screens/devices if systems are unattended.

**7.6 Managing the Safety of our Website**

* We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
* Personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
* The administrator account for our website will be secured with an appropriately strong password.
* We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

**7.7 Publishing Images and Videos Online**

* We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: GDPR, child protection, and behaviour management policy.

**7.8 Managing Email**

* Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, GDPR and the code of conduct/behaviour policy.
  + The forwarding of any chain messages/emails is not permitted.
  + Spam or junk mail will be blocked and reported to the email provider.
  + Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  + Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
* Members of staff will immediately tell the leadership team if they receive offensive communication, and this will be recorded in our safeguarding files/records.

**7.8.1 Staff email**

* The use of personal email addresses by staff for any official setting business is not permitted.
  + All members of staff will use the settings email address for all official communication.

**7.9 Educational use of Videoconferencing and/or Webcams**

* We recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning and communication benefits.
  + All videoconferencing will be switched off when not in use and will not be set to auto-answer.
  + Only official and secure videoconferencing platforms will be used, these include Microsoft Teams, Zoom & Skype Business. In setting up or accessing videoconferencing there must be a secure link or code shared with relevant parties in advance and must contain a secure password or encrypted channel to ensure only those required can access/join the conference call.
  + Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

**7.10 Management of Applications (apps) used to Record Children’s Progress**

* We use Tapestry to track learner’s progress and share appropriate information with parents and carers.
* Claire Elliott-Hare is ultimately responsible for all data, she ensures that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
* To safeguard learner’s data:
  + Only approved software and devices will be used for recording and storing learners’ personal details, attainment or photographs.
  + All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  + Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

**8 Access Privileges**

We ensure robust access privileges to keep personal data secure.

Our setting has access to a Wi-Fi Network. The Wi-Fi system at Squirrel Lodge Nursery is independent of the server to reduce the risk of hacking or a data breach. Wi-Fi details are available through speaking to a member of staff at reception.

In order to gain access to our systems all new employees must speak to their line manager.

Access to our databases and systems are limited to those who need it, line managers will approve employee requests to gain access to these systems. In order to use any database or system an employee must undertake basic training of that system and read this policy to ensure compliance.

**9 Disposal of ICT equipment**

When ICT equipment needs to be disposed of, we delete and shred all personal data saved to the local hard drive of that system, where applicable all equipment will be reset to factory settings. Once data on ICT equipment is fully deleted. We will use an accredited third party disposal company, who issue a disposal certificate listing all equipment that has been disposed of.

Depending on the type of ICT equipment being disposed of, internal disposal options maybe more appropriate, operational managers will decide the best way to dispose of the ICT equipment they use.

**10 Use of Portable Data Storage Media**

Portable data holding devices such as flash drives/USB sticks are vulnerable to being lost if great care is not taken to ensure that they are kept safe and secure. They can hold any kind of electronic data some of which could be sensitive regarding the individuals we work with. If lost or stolen there is a risk that such data could be accessed by unauthorised individuals.

For all data controlled by Squirrel Lodge Nursery:

* If data needs to be held on a portable data storage device, then it must only be held on an encrypted, password protected device belonging to Squirrel Lodge Nursery
* Personal or any other device not belonging to the company must not be used to store data;
* Staff needing to use a portable data storage device drive must request one from Squirrel Lodge Nursery
* All staff issued with a device must ensure it has a secure password and take all reasonable steps to ensure that the device is not lost or stolen.
* All devices issued to staff will remain the property of Squirrel Lodge Nursery and must be returned when no longer needed by the staff member for work purposes.
* All staff issued with a device must not reveal the password of the device to anyone not employed by Squirrel Lodge and only to fellow employees on a need-to-know basis;
* Any member of staff issued with a device must change the password on the device if they believe that someone else may have learnt the password and/or after it has been shared with another member of staff and their need to access that data has ceased.
* Any member of staff leaving our employment will be required to ensure that they return any device that they have been issued with.

**10.1. Bring Your Own Device (BYOD) & Working from Home**

From time to time, Squirrel Lodge Nursery allows employees to use BYOD to complete training whilst at work subject to line manager approval. **It is forbidden to transfer documents/files from our servers onto other storage media or systems not owned or controlled by Squirrel Lodge Nursery.** The setting accepts no liability in respect of any loss/damage to personal ICT devices. The decision to bring and use a personal ICT device is your responsibility, as does the liability for any loss/damage that may result from the use of a personal ICT device.

Staff working from home must ensure:

* The security is always up-to-date.
* **Third parties do not have access to devices and its contents.**
* If your PC / Laptop has a security breech i.e. virus, malware, data corruption, etc. please speak to your manager asap, and do not use it for work purposes, until this is fully resolved
* Work content is not saved to personal PC / Laptop
* Only certified and licensed software i.e. Microsoft, Symantec, etc. is used

**10.2 Theft of ICT Equipment**

- Break-in – securing offices, rooms, passwords

- Left unattended – locking screens, securing office

- Snatched – locked, unable to get access,

- Members of staff – usage policy

**10.3 Responding to Online Safety Incidents and Concerns**

* All members of staff will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery, cyberbullying and illegal content.
* All members of staff must respect confidentiality and the need to follow the official procedures for reporting concerns.
  + Service users and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
* We require staff, parents/carers to work in partnership to resolve online safety issues.
* After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
* If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.
* Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.

**11.1 Concerns about Learners Welfare**

* The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
  + The DSL (or deputy) will record these issues in line with our child protection policy.
* The DSL (or deputy) will ensure that any concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Multi-agency Partnership’s thresholds and procedures.
* We will inform parents and carers of incidents or concerns involving their child, as and when required.

**11.2 Staff Misuse**

* Any complaint about staff misuse will be referred to the Management Team, where the allegations policy will be followed.
* Any allegations regarding a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).
* Appropriate action will be taken in accordance with our staff code of conduct.

**11.3 Cyberbullying and sharing nude and semi-nude imagery:**

Squirrel Lodge Nursery will not tolerate any forms of cyberbullying and/or sharing nude and semi-nude imagery. Upon being notified of any concerns we will follow our safeguarding procedures.  We encourage good behaviour and aim to prevent all forms of bullying amongst children, staff and the wider community. If the form of bullying moves towards harassment or threatening behaviour or communications we will contact the police as it could become a criminal offence.

Further details on cyberbullying can be accessed: <https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/cyberbullying>. In relation to sharing nude and semi-nude imagery we follow: [https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people](https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people%20%20)  and

KSCMP guidance: <https://www.kscmp.org.uk/__data/assets/word_doc/0008/148904/Kent-and-Medway-Responding-to-Nude-and-Semi-Nude-Image-Sharing-Guidance-V2.docx>

**12.** **Procedures for Responding to Specific Online Incidents or Concerns**

**12.1 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)**

* We will ensure that all members of staff are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
* We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
* We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for children, staff and parents/carers.
* We will ensure that all members of staff, parent/carers are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
* If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  + Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board’s procedures.
  + If appropriate, store any devices involved securely.
  + Make a referral to Children’s Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
  + Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
  + Inform parents/carers about the incident and how it is being managed.
  + Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
  + Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
* We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
  + Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: [www.ceop.police.uk/safety-centre/](http://www.ceop.police.uk/safety-centre/)
* If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
* If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](https://www.kent.police.uk/advice/advice-and-information/caa/child-abuse/) (CSET) by the DSL (or deputy).
* If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

**12.2** **Indecent Images of Children (IIOC)**

* We will ensure that all members of staff are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
* We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
* We will seek to prevent accidental access to IIOC by using an internet Service provider which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
* If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
* If made aware of IIOC, we will:
  + Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
  + Store any devices involved securely.
  + Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
* If made aware that a member of staff or a child has been inadvertently exposed to indecent images of children, we will:
  + Ensure that the DSL (or deputy) is informed.
  + Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](https://www.iwf.org.uk/) .
  + Ensure that any copies that exist of the image, for example in emails, are deleted.
  + Report concerns, as appropriate to parents and carers.
* If made aware that indecent images of children have been found on the setting provided devices, we will:
  + Ensure that the DSL (or deputy) is informed.
  + Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](https://www.iwf.org.uk/) .
  + Ensure that any copies that exist of the image, for example in emails, are deleted.
  + Inform the police via 101 (999 if there is an immediate risk of harm) and Children’s Social Work Service (as appropriate).
  + Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  + Report concerns, as appropriate to parents and carers.
* If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  + Ensure that the DSL is informed in line with our managing allegations against staff policy.
  + Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  + Quarantine any devices until police advice has been sought.

**12.3 Cyberbullying**

* Cyberbullying, along with all other forms of bullying, will not be tolerated.
* Full details of how we will respond to cyberbullying are set out in other relevant policies.

**12.6 Online Hate**

* Online hate content, directed towards or posted by, specific members of staff will not be toleratedandwill be responded to in line with existing policies, including anti-bullying and behaviour management.
* All members of staff will be advised to report online hate in accordance with relevant policies and procedures.
* The Police will be contacted if a criminal offence is suspected.
* If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.

**12.7 Online Radicalisation and Extremism**

* We will take all reasonable precautions to ensure that children and staff are safe from terrorist and extremist material when accessing the internet on site. We have various software on our server that will support blocking threats and exposed content.
* If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
* If we are concerned that member of staff may be at risk of radicalisation online, the DSL (or Deputy) will be informed immediately, and action will be taken in line with the child protection and allegations policies.

1. **Policy Breaches and Reporting Concerns**

Participants are encouraged to report any Online Safety Concerns, this includes data breaches, social media concerns, online concerns, inappropriate language or behaviour takes place during online streaming/content. Any participants involved will be removed by staff, and the session may be terminated.

All participants are expected to behave in line with existing policies and expectations. Zero tolerance will be taken to those who do not adhere to the standards required. This includes staff and participants. Failure to adhere to our standards will result in staff/participants being suspended from using our services initially whilst an investigation is undertaken. This could result in dismissal or being removed and blocked from using our services, and in extreme cases the police may also be involved.

Inappropriate online behavior will be responded to in line with existing policies such as safeguarding, code of conduct, allegations against staff, anti-bullying and behavior.

All issues should be raised to Claire Elliott-Hare [squirrellodgenursery@hotmail.com](mailto:squirrellodgenursery@hotmail.com)

1. **Useful Links for Educational Settings**

**Kent Support and Guidance for Educational Settings**

**Education Safeguarding Team**:

* Online Safety Tel: 03301 651500
* Guidance for Educational Settings:
  + <https://www.kelsi.org.uk/child-protection-and-safeguarding>

**KSCMP:**

* <https://www.kscmp.org.uk/>

**Kent Police:**

* [www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)

Inan emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

**Other:**

* Kent Public Service Network (KPSN): [www.kpsn.net](http://www.kpsn.net)

**National Links and Resources for Educational Settings**

* CEOP:
  + [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
  + [www.ceop.police.uk](http://www.ceop.police.uk)
* Childnet: [www.childnet.com](http://www.childnet.com)
* Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
* Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
* Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
* NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
  + ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
  + Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
* The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk/)
* UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
  + Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
* 360 Safe Self-Review tool for schools: [www.360safe.org.uk](http://www.360safe.org.uk/)

**National Links and Resources for Parents/Carers**

* Action Fraud: [www.actionfraud.police.uk](http://www.actionfraud.police.uk/)
* CEOP:
  + [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
  + [www.ceop.police.uk](http://www.ceop.police.uk)
* Childnet: [www.childnet.com](http://www.childnet.com)
* Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org/)
* Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
* Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
* Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
* NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
  + ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
  + Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
* The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk/)
* UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

**Appendix 1 - Parent/Carer/Child Acceptable Use of Technology Policy (AUP) Declaration**

1. I know that my child will from time to time have supervised access to the internet in order to support their learning and development whilst at the setting.
2. I am aware that use of mobile and smart technology, such as mobile phones by parents/carers, staff and visitors is not permitted within our nursery areas or childcare regulated activities.
3. I understand that the setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use setting devices under supervision. I understand that the setting cannot ultimately be held responsible for the nature and content of materials accessed online.
4. I am aware that my child will receive age appropriate online safety education to help them understand the importance of safe use of technology and the internet, both in and out of the setting.
5. I have read the settings Online Safety Policy (this can be found on our website) [www.squirrellodgenursery.com](http://www.squirrellodgenursery.com)
6. I will support the settings safeguarding policies and will ensure that I use appropriate parental controls, will appropriately supervise/monitor my child’s use of the internet outside of the setting and will discuss online safety with them when they access technology at home.
7. I know I can seek support from the setting about online safety, to help keep my child safe online at home.
8. I will support the setting approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.
9. I will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the setting community, or content that could adversely affect the reputation of the setting
10. I understand that a partnership approach to online safety is required. If the setting has any concerns about either my or my child’s safety online, then I will be contacted.
11. I understand that if I do not abide by the settings policy, appropriate action will be taken. This could include sanctions being applied in line with the setting policies, and if a criminal offence has been committed, the police being contacted.
12. I know that I can speak to the Designated Safeguarding Lead in the setting if I have any concerns about online safety.

**I have read, understood and agree to comply with the online safety policy, which includes the acceptable use of Technology, Mobile and Smart Technology and Social Media.**

Child’s Name……………………………………

Date………………………………………………

Parent/Carer’s Name……………………………………………………....................................

Parent/Carer’s Signature………………………………………………... Date…………………………….

**Appendix 2 - Employee Recognition**

Our Online Safety policy has been developed in accordance with the principles established by the Children Acts 1989 and 2004 and related guidance. This includes but not limited to;

* DfE statutory guidance ‘[Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)’ 2023,
* [Early Years and Foundation Stage](https://www.gov.uk/government/publications/early-years-foundation-stage-framework--2) 2024
* ‘[Working Together to Safeguard Children](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2)’ 2023
* [Kent Safeguarding Children Multi-Agency Partnership](http://www.kscb.org.uk)
* Inspecting safeguarding in early years, education and skills settings (2023)
* The Local Authority Exemplar guidance on acceptable use of technology and mobile and smart technology and social media policies.

The Management at Squirrel Lodge Nursery take seriously our responsibility to promote the welfare and safeguard all the children entrusted to our care.

As part of our ethos we are committed to:

* Maintaining children’s welfare as our paramount concern
* Safeguarding children - the action we take to promote the welfare of children and protect them from harm - is everyone’s responsibility.
* Providing an environment in which children feel safe, secure, valued and respected; confident to talk openly and sure of being listened to
* Using technology to support children’s learning in a safe and controlled environment.
* Not use nursery phones, tablets, laptops or computers for personal use.
* Understanding the risk associated with online safety, smart technology, mobile phones and social media, alongside the requirements to safeguard children at all times.
* Working with parents to build an understanding of the responsibilities to ensure the welfare of all children including the need for referral to other agencies in some situations.

As an employee/ volunteer/ student of Squirrel Lodge Nursery, I have read the Online Safety Policy and understand, accept and will comply with its contents as part of my contract of employment.

I understand that this policy may be altered from time to time and that I will be kept informed of any changes therein.

Signature...................................................….

Print Name..................................................................

Date...............................................................

# Appendix 3 Acceptable Use of Technology for Staff, students and Volunteers

### Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Squirrel Lodge Nursery IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for children, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Squirrel Lodge Nursery expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that the setting systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

**Policy scope**

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the setting or accessed by me as part of my role within Squirrel Lodge Nursery professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**.**
2. I understand that Squirrel Lodge Nursery’s Acceptable Use of Technology Policy (AUP) should be read and followed in line with the setting’s child protection and online safety policy and staff code of conduct.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the setting ethos, setting staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

**Use of setting** **devices and systems**

1. I will only use the equipment and internet services provided to me by the setting for example when using setting provided laptops, tablets, mobile phones and internet access, when working with children or for carrying out work.
2. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Personal use of setting IT systems and/or devices by staff is not allowed. I understand that I can access the internet from my own devices on my break or out of work hours, so long as I am not accessing anything unsafe or that would cause a safeguarding concern for the workplace.

**Data and system security**

1. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
   * I will protect the devices in my care from unapproved access or theft, for example, by not leaving devices visible or unsupervised in public places.
2. I will respect the setting system security and will not disclose the password or security information to others.
3. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the manager.
4. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the manager.
5. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the setting information security policies.
   * All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
   * Any data being removed from the setting site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the setting.
6. I will not keep documents which contain setting related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. I will use the setting learning platform to upload any work documents and files in a password protected environment.
7. I will not store any personal information on the setting IT system, including setting laptops or similar devices, that is unrelated to the settings activities, such as personal photographs, files or financial information.
8. I will ensure that setting owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
9. I will not attempt to bypass any filtering and/or security systems put in place by the setting.
10. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the owner/manager as soon as possible.
11. If I have lost any setting related documents or files, I will report this to the manager/ owner as soon as possible.
12. Any images or videos of children will only be used as stated in the setting camera and image use policy (see policy folder). I understand images of children must always be appropriate and should only be taken with setting provided equipment and only be taken/published where children and/or parent/carers have given explicit written consent.

**Teaching practice**

1. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Squirrel Lodge Nursery as detailed in the child protection and online safety policies, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
2. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL in line with the setting child protection and online safety policies.
3. I am aware of the expectations relating to safe technology use in the nursery and other working spaces as listed in our child protection and online safety policies.
4. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
   * exploring age-appropriate online safety principles as part of the curriculum and reinforcing safe behaviour whenever technology is used.
   * creating a safe environment where children feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
   * Informing the DSL if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
   * make informed decisions to ensure any online safety resources used with children is appropriate.
5. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

**Mobile devices and smart technology**

1. I have read and understood the setting’s mobile and smart technology and social media policies which addresses use by children and staff.
2. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct and the setting mobile technology policy and the law.

**Online communication, including use of social media**

1. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection policy, online safety policy, staff code of conduct, social media policy and the law.
2. As outlined in the staff code of conduct and setting social media policy:
   * I will take appropriate steps to protect myself and my reputation, and the reputation of the setting, online when using communication technology, including the use of social media.
   * I will not discuss or share data or information relating to children, staff, setting business or parents/carers on social media.
   * I will set my social media accounts as private
3. My electronic communications with current and past children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
   * I will ensure that all electronic communications take place in a professional manner via setting approved and/or provided communication channels and systems, such as a setting email address, tapestry account or telephone number.
   * I will not share any personal contact information or details with families such as my personal email address, phone number or social media account.
   * I will not add or accept friend requests or communications on personal social media with current or past children and/or their parents/carers.
   * If I am approached online by a current or past child or their parents/carers, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
   * Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or manager on a case-by-case basis. The advice will be that unless you are related to them, you should not be friends with them on social media.

**Policy concerns**

1. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
2. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate, or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
3. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the setting into disrepute.
4. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the setting child protection policy.
5. I will report concerns about the welfare, safety, or behaviour of staff online to the manager, in line with the setting child protection policy and/or the allegations against staff policy.

**Policy Compliance and Breaches**

1. If I have any queries or questions regarding safe and professional practise online, either in the setting or off site, I will raise them with the DSL and/or the manager.
2. I understand that the setting may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all setting provided devices and setting systems and networks including setting provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via setting provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
3. I understand that if the setting believe that unauthorised and/or inappropriate use of setting devices, systems or networks is taking place, the setting may invoke its disciplinary procedures as outlined in the staff code of conduct and disciplinary policy.
4. I understand that if the setting believe that unprofessional or inappropriate online activity, including behaviour which could bring the setting into disrepute, is taking place online, the setting may invoke its disciplinary procedures as outlined in the staff code of conduct and disciplinary procedures.
5. I understand that if the setting suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Squirrel Lodge Nursery’s** **Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.**

Name of staff member: ……………………………………………………………………………………

Signed: ………………………..........................................................................................................

Date (DDMMYY)……………………………………………………………………………………….…...

### Appendix 4. Visitor Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help Squirrel Lodge Nursery ensure that all visitors understand the setting’s expectations regarding safe and responsible technology use.

**Policy scope**

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, accessed by me as part of my role within Squirrel Lodge Nursery professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**.**
2. I am aware that this AUP does not provide an exhaustive list; visitors should ensure that all technology use is consistent with the setting ethos, setting safeguarding policies, national and local education and child protection guidance, and the law.
3. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
4. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
5. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the setting into disrepute.

**Data and image use**

1. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.
2. I understand that I am not allowed to take images or videos of children unless I am a photographer/ videographer specifically hired for an event or photo shoot and specific consent has been sought. Any images or videos of children will only be taken in line with the setting camera and image use policy.

**Nursery practice**

1. I am aware of the expectations regarding safe use of technology in the nursery and other working spaces, including appropriate supervision of children.
2. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the children.
3. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the setting community, I will report this to the DSL, in line with the setting child protection/ online safety policy.
4. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

**Use of mobile devices and smart technology**

12. In line with the setting mobile and smart technology policy, I understand that:

* Mobile phone, smart watches and other personal devices are not permitted in the Nursery area, they will be kept in the office safe.
* Appropriate signage and information are in place when signing in to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology.
* Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.
* If visitors require access to mobile and smart technology, for example when working with children as part of multi-agency activity or during an LA visit or OFSTED inspection, the DSL/ Manager will discuss this with the visitor prior to use being permitted.
* Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the setting on a Visitor AUP, Appendix 4. This may include undertaking appropriate risk assessments if necessary.
* Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or manager of any breaches of our policy.

**Policy compliance, breaches or concerns**

13. If I have any queries or questions regarding safe and professional practice in the setting or online either in the setting or off site, I will raise them with the Designated Safeguarding Leads Terrie Platt or Rebecca Hutton or Claire Elliott-Hare.

14. I understand that if the setting suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Squirrel Lodge Nursery’s Visitor Acceptable Use of Technology Policy when using the internet and other associated technologies.**

Name of visitor: …………………………………………………………………...……………

Signed: ………………………...........................................................................................................

Date (DDMMYY)………………………………………………............................................................................