Sir James Knott Nursery School

Online Safety Policy

“Resilient, reflective, respectful”

Certified as reviewed and approved by the Curriculum and Safeguarding Committee:	**23rd May 2022**
Adoption by Full Governing Body:	**11th July 2022**
Designated member of staff’s responsibility:	**Mr Croft- Headteacher**
Next review date:	**September 2023 or earlier if new guidance becomes available**

Online Safety Policy

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between 'Key School Leads'. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (2021 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It is designed to sit alongside our statutory Safeguarding and Child Protection Policy. Any issues or concerns with online safety **must** follow the schools safeguarding and child protection procedures.

Designated Safeguarding Lead	John Croft
Online Safety Lead	John Croft
Online Safety/ Safeguarding Governor	Linsey Garr
Computing Lead	John Croft
Network Manager/ other technical support	Nicki Battensby/ Babble

The policy will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Pat of school induction pack for **all** new staff (including temporary, supply and non-classroom based staff)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policy (AUP) for staff, volunteers, contractors, Governors, pupils and parents/carers.

This policy aims to:

- Set out expectations for all community members online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/ digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibility with technology and the online world:

- For the protection and benefit of the children and young people in their care, and
- For their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- For the benefit of the school, supporting the school's ethos, aims and objectives, and protecting the reputation of the school and profession.

- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Relationship Policy.

Key responsibilities: Headteacher and Online Safety Lead

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Ensure that policies and procedures are followed by staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships.
- Liaise with the Designated Safeguarding Lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Govenors to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event pf a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised.
- Ensure that there is a system in place to monitor and support staff (e.g. Network Manager) who carries out internal technical online-safety procedures.
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements.
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Ensure that online safety education is embedded across the curriculum in line with the Revised EYFS framework.
- Promote an awareness of an commitment to online safety throughout the school community, with a strong focus on parents.
- Communicate regularly with SLT and the designated safeguarding committee to discuss current issues (anonymized), review incident logs and filtering/ change control logs and discuss how filtering and monitoring work and have been functioning/ helping.

Key responsibilities: Computer Lead

- Embed consent, mental well-being, healthy relationships and staying safe online into the PSHE/ Relationships education and curriculum. “This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, staff will address online safety and appropriate behaviour in an age appropriate way that is relevant to pupils lives”.
- For Computer Lead and staff to support parents with how to make online safety safer for their child/ children.
- Work closely with DSL, Online-Safety/ Safeguarding Governor and all other staff to ensure an understanding of the issues, approaches and messages within the PSHE/ relationships curriculum.

Technical- infrastructure/ equipment, filtering and monitoring:

The school and Babble will be responsible for ensuring that the school infrastructure/ network is as safe and secure as it reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensures the school meets recommended technical requirements.

There will be regular reviews and audits of the safety and security of school technical systems.

Servers, wireless systems and cabling must be securely located and physical access restricted.

All users will gave clearly defined access rights to school technical systems and devices.

All users will be provided with a username and secure password. John Croft will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly.

The “master/ administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place.

Nicki Battensby is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Contents lists are regularly updated and internet use is logged and regularly monitored.

There is a clear process in place to deal with requests for filtering changes.

The school and Babble have provided enhanced/ differentiated user-level filtering.

The Network Manager and Babble regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

An appropriate system is in place for users to report any actual. Potential technical incident/ security breach to the relevant person, as agreed.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.

The school infrastructure and individual workstations are protected by up to date virus software.

An agreed policy is in place for the provision of temporary access of 2guests2 (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

An agreed policy is in place regarding the extent of personal use that users (staff/ pupils/ community users) and their family members are allowed on school devices that may be used out of school.

Use of Mobile Phones in School:

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours.
- Sir James Knott Nursery School allows staff to bring in personal mobile telephones and devices for their own use, in their own time, away from children.
- Staff bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All staff must ensure that their mobile telephone/devices are left inside their bag throughout contact time with children. Staff bags should be placed in their locker or staffroom.
- Mobile phone calls may only be taken during staff breaks or in staff members own time.
- **It is not acceptable for any member of staff to take a photograph in the school on their personal mobile phones.**
- If staff have a personal emergency they are able to use their mobile telephone, with permission from the Headteacher.
- If any staff members has an family emergency or similar, they are permitted to give the telephone number of the school office to family members/ partners/ children.
- Staff need to ensure that the Headteacher has up to date contact information and that staff make their families. Children's schools etc, aware of the emergency work telephone numbers. This is the responsibility of the individual staff member.
- **Volunteers, contractors, Governors** should leave their phones in their pockets, on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos- unless with permission from the Headteacher/ Online Safety Lead.

Digital Images:

The use of digital images must depend upon the appropriate permission given by parents. All photographs/ videos should be taken on a school device and once uploaded/ emailed, deleted from the device.

Training- School Staff

All school staff receive an online safety update at least once each half term, access to Safer Schools, regular e mails and bulletins. It is the responsibility of the Online Safety Lead to ensure that school staff have the most up to date training and information.

Training- Governor

Regular updates during meetings, reports of online safety data and relevant training.

Training- Parents

May parents and carers may only have a limited understanding of online safety risks and issues, yet they plan an essential role in the education of their children and in the monitoring/ regulation of the children's on-line behavours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through: *** Curriculum activities * Letters, newsletters, website- Parents/ Carers evenings/ Sessions, campaigns e.g. Safer Internet Day * Webinars.**

Reporting Online Safety Concerns:

Staff- Report to DSL or Online Safety Lead via our current written form. (Looking into the purchase of CPoms).

Children- Report to an adult who will then follow the above process.

Parents- Report to a member of staff who will then seek advice from the DSL or Online Safety Lead.

Additional Resources

https://www.ceop.police.uk/Safety-Centre/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://www.childnet.com/

https://nationalonlinesafety.com/