Sir James Knott Nursery School

E- Safety Policy

"Creating strong and lasting foundations for learning"

Certified as reviewed and approved by the Teaching and Learning Sub-Committee:	**22nd January 2019**
Adoption by Full Governing Body:	**11th March 2019**
Designated member of staff's responsibility:	**Mr Croft- Headteacher**
Next review date:	**September 2020 or earlier if new guidance becomes available**

E- Safety Policy

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside of school. Electronic communication helps staff and children learn from each other. These technologies can provide a toolkit for sharing learning experiences with parents (for example through Tapestry), stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Schedule for Development/ Monitoring/ Review

This E-Safety Policy has been developed by the E-Learning Lead (currently Headteacher).

This E-Safety Policy was approved by the Governing Body:	22nd January 2019
The implementation of this E-Safety Policy will be monitored by the:	E- Learning Lead (currently Headteacher), Class Teachers, Teaching Assistants
Monitoring will take place at regular intervals:	ICT Technician from Stephenson Memorial Primary School on a termly basis.
The Teaching and Learning Governors Sub-Committee will receive a report on the implementation of the E-Safety Policy generated by the E-Learning Lead (currently Headteacher) (which will include anonymous details of e-safety	Governing Body Meetings

incidents) at regular intervals:	
The School uses North Tyneside Council filtering systems which blocks sites that fall into categories such as pornography, racial hatred extremism, gaming, sites of an illegal nature etc. The school will work with North Tyneside Council and the Schools Broadband team or broadband/ filtering provider to ensure that the filtering policy is continually reviewed.	If staff or children discover unsuitable sites, the URL will be reported to the Schools Designated Safeguarding Lead and will then be recorded and escalated as appropriate. Regular checks are made to ensure that the filtering methods selected are effective and appropriate in collaboration with the ICT technician from Stephenson Memorial Primary School and we seek advice from North Tyneside Council. Any material that the schools believes is illegal will be reported to appropriate agencies such as Internet Watch Foundation (IWF), Police or Child Exploitation and Online Protection Centre (CEOP) immediately.
The E- Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2020

Scope of the Policy

This policy applies to all members of the school community (including staff, students, parents/carers and volunteers), who have access to and are users of school ICT systems, both in and out of school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies.

The school will monitor the impact of the policy using

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Headteacher and Leadership Team:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E- Learning Lead (currently Headteacher).
- The Headteacher is responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Leadership Team will receive regular feedback from the E- Learning Lead (currently Headteacher) in relation to parental involvement/usage of Seesaw (online learning journal).
- The E- Learning Lead (currently Headteacher) should be aware of the procedures to be followed in the event of a serious allegation being made against a member of staff.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to provide support to those colleagues who take on important monitoring roles.
- The Headteacher will ensure that parents attention is drawn to the E-Safety Policy in newsletters, parent e-mails and on the school website.

E- Learning Lead (currently Headteacher):

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Provides training and support for staff.
- Liaises with ICT technical staff.
- Manages all parental permissions and logins for Seesaw.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Technical Support:

- Are responsible for ensuring that the school's technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets the required e-safety technical requirements and any Local Authority Policy that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network/ internet/ e mail is regularly monitored in order that any misuse/ attempted misuse can be reported to the Headteacher for investigation/ action/ sanction.
- That no filters are removed without the authorisation of the Headteacher who will ensure that all implications are considered to ascertain the reason for filtering.
- That monitoring software/ systems are implemented and updated.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school E-Safety Policy and practices.
- That they have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP).
- They report any misuse or problem to the E-Learning Lead (currently Headteacher)

for investigation/action/sanction.

- All digital communications with staff and parents should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Children understand (at an age appropriate level), and follow the e-safety and acceptable use policies.
- Staff monitor the use of digital technologies, mobile devices and cameras etc. and implement current safeguarding polices with regard to these devices.

Child Protection / Safeguarding Designated Person / Officer

School should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Access to parents' sections of the school website
- Sharing information on Seesaw (online learning journal)
- The 'No mobile phone' message to safeguard vulnerable children/people on site

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. We will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information on local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate usage of:

- Digital and video images taken at school events.
- Access to parents' sections of the website
- Seesaw online learning journal

Policy Statements

Education - Children

Children will be educated in e-safety at an appropriate level, and will be taught to notify staff if they are unsure. Children have been involved in the creation of an e-safety leaflet which has been shared with parents and highlights the main issues for this age group.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

Children will be reminded about e-safety during key group times as part of SEALS and also during research based work such as floor books, where the internet is used as a research tool to acquire information.

Education — Parents/Carers

The school provides information to parents/carers through:

- Letters, newsletters, emails, texts
- Parents consultations
- Reference to safe websites/apps to support their child’s learning at home.
- As with other aspects of safeguarding, e-safety is everyone’s responsibility.

Education — Staff/ Volunteers

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. These are also available digitally for them to access in google drive, on school iPads.

Training will be offered as follows:

- E-safety training will be made available to staff.
- New staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use

Policies.

- This E-Safety Policy will be shared with staff and updates will be emailed and shared on google drive.
- The E-Learning Lead (currently Headteacher) will receive regular updates through attendance at external training events (e.g. Local Authority or other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings/ Teacher Training days.
- The E- Learning Lead (currently Headteacher) will provide advice/ guidance/ training to individuals as required.
- This policy will operate in conjunction with other school policies such as the Relationship Policy, Safeguarding and Child Protection Policy, and Staff Code of Conduct and Behaviour Policy.

Training — Governors

Governors should take part in e-safety training/ awareness sessions, with particular importance for those who are members of any sub-committees involved in technology, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisations.
- Participation in school training/ information sessions for staff or parents.

Keeping Children Safe in Education September 2018

Schools are required "to ensure children are safe from terrorist and extremist materials when accessing the internet in school, including by establishing appropriate levels of filtering" ***(Revised Prevent Duty Guidance: for England and Wales, 2015).***

In line with Keeping Children Safe in Education, September 2018, Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the risks from the school's IT system. As part of this process, Governing Bodies and proprietors should ensure their school has appropriate filters and monitoring systems in place.

The school follows advice from UK Safer Internet Centre in relation to;

- Appropriate filtering
- Appropriate Monitoring
- Provider responses
- Provider checklists

https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Technical- infrastructure/ equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/ network is as safe and secure as is 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 e-safety responsibilities:

- School technical systems will be managed in ways that ensure that 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 have clearly defined access rights to school technical systems and devices.
- The E-Safety Lead/ Headteacher are 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.
- The school receives termly visits from an ICT Technician from Stephenson Memorial Primary School from Spring Term 2019 who monitors 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, mobile devices etc. from accidental or malicious attempts which might threaten the security of the schools systems and data.

Use of digital and video images — Photographic and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff need to be aware of the risks associated with sharing images and with posting digital images on the internet. In school, this would be restricted to the school website and Seesaw, both of which require parental consent.

- Staff are allowed to take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of these images.
- Photographs published on the schools' website will be carefully selected and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on the school website, particularly in association with photographs.
- We maintain a list of children whose parents do not wish their image to appear on our school website, local media, or on another child's Seesaw account. This list is available from the school office, and all staff have an awareness of this in relation to their own class/es. These photographs may be used on the child's own Seesaw accounts or for classroom use only.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date

- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Staff must ensure that they comply with the Data Policy by:

- At all times taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Using personal data only on secure, password protected computers and other devices, ensuring they are properly 'logged off' at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.

Google Drive

The Schools uses Google Drive to share key publications, planning formats, records for staff across the teaching and learning team and for Governors. Most staff access their files through the Google Drive app on their work iPad. This ensures that all staff and Governors have the key documentation in order to fulfil their roles and responsibilities.

Google Drive offers access to files anywhere through secure cloud storage and file backup. The goal of the Whitepaper is to provide a document on its efforts and commitments regarding security and privacy.

https://cloud.google.com/security/whitepaper

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication technologies	Allowed	Not allowed
Mobile phones may be brought into school	✓ Locked away and only used in staffroom or classroom when no children are present.	
The use of mobile phones in lessons		✓
Use of mobile phones in social time	✓	
Taking photos on mobile phones		✓
Use of handheld devices (iPads)	✓ Only able to used allocated Work iPad.	
Use of personal email address in school, or on school network		✓
Use of school email for personal emails		✓
Use of messaging apps		✓

When using communication technologies, the school considers the following as good practice:

- The office school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the Headteacher—in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and/or parents/carers must be professional in tone and content. These communications may only take place on official school systems and not on personal email accounts.

Social Media- Protecting Professional Identity

All Schools and Local Authorities have a duty of care to provide a safe learning environment for children and staff. Schools and Local Authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or Local Authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk Assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to children, parents/ carers or school staff.
- They do not engage in online discussion on persona matters relating to members of the school community.
- Personal Opinions should not be attributed to the school or Local Authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

ICT and Prevent

Statutory Duties:

The duty to prevent children and young people being radicalised is set out in the following
documents:

- Counter Terrorism and Security Act 2015
- Keeping Children Safe in Education 2018
- Prevent Duty Guidance 2015
- Working Together to Safeguard Children 2018

Non-statutory Guidance:

Promoting fundamental British Values as part of SMSC in schools:

- DfE Departmental advice for maintained schools 2014

Aims and Principles:

Sir James Knott Nursery School Preventing Extremism and Radicalisation Policy is intended to provide a framework for dealing with issues relating to vulnerability, radicalisation and exposure to extreme views. We recognise that we are well placed to be able to identify safeguarding issues and this policy sets out how the school will deal with such incidents and identifies how the curriculum and ethos underpins our actions.

The objectives are that:

- All Governors, Teachers, Teaching Assistants and Non-Teaching Staff will have an understanding of what radicalisation is and why we need to be vigilant in school.
- All Governors, Teachers, Teaching Assistants and Non-Teaching Staff will know what the school policy is on tackling extremism and radicalisation and will follow policy guidance swiftly when issues arise.
- All children will understand the dangers of radicalisation and exposure to extremist views at an age appropriate level; building resilience against these and knowing what to do if they experience them.
- All parents/carers and children will know that the school has policies in place to keep children safe from harm and that the school regularly reviews its systems to ensure they are appropriate and effective.

The main aims of this policy are to ensure that staff are fully engaged in being vigilant about radicalisation; that they overcome professional disbelief that such issues will not happen here and ensure that we work alongside other professional bodies and agencies to ensure that our children are safe from harm.

Recognising the indicators of vulnerability to radicalisation:

There is no such thing as a “typical extremist”: those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

Children may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. There are no known definitive indicators that a young person is vulnerable to radicalisation, but there are a number of signs that together increase the risk and it is vital that school staff are able to recognise these.

Signs of vulnerability include:

- Underachievement
- Being in possession of extremist literature
- Poverty
- Social exclusion
- Traumatic events
- Global or national events
- Religious conversion
- Changes in behaviour
- Extremist influences
- Conflict with family over lifestyle
- Confused identity
- Victim or witness to race or hate crimes
- Rejection by peers, family social groups or faith

Recognising Extremism:

There are a number of behaviours that may indicate a child is at risk of being radicalised or exposed to extreme views.

These include:

- Showing sympathy for extremist causes
- Making remarks or comments about spending time in the company of other suspected extremists
- Out of character changes in dress, behaviour and peer relationships, (there are powerful narratives, programmes and networks that young people can come across online, so involvement with particular groups may not be apparent)

- Possession of materials or symbols associated with an extremist cause
- Attempts to impose extremist views or practices on others
- Communications with others that suggest identification with a group, cause or ideology
- Secretive behaviour
- Intolerance of difference, including faith, culture, gender, race or sexuality
- Graffiti, artwork or writing that displays extremist themes
- Using insulting or derogatory names for another group
- Increase in prejudice-related incidents committed by that person – these may include:
- Physical or verbal assault
- Provocative behaviour
- Damage to property
- Derogatory name calling
- Possession of prejudice-related materials
- Prejudice related ridicule or name calling
- Inappropriate forms of address
- Refusal to co-operate
- Attempts to recruit to prejudice-related organisations
- Condoning or supporting violence towards others, especially to other faiths or cultures

Any prejudice, discrimination or extremist views, including derogatory language, displayed by children or staff will always be challenged and where appropriate dealt with in line with our Relationship Policy for pupils and the Code of Conduct and Behaviour for staff.

Curriculum:
We are committed to ensuring our pupils are offered a broad and balanced curriculum that aims to prepare them for life in modern Britain. We encourage our pupils to be inquisitive learners who are open to new experiences and are tolerant of others.

Our school ethos supports the development of the whole child as a reflective learner within a safe, respectful learning environment. Teaching the schools' core values alongside the fundamental British values supports quality teaching and learning, whilst making a positive contribution to the development of a just, fair and civil society.

We will also work with local partners, families and communities in our efforts to challenge extremist views and to assist in the broadening of our children's experiences and horizons.

Links to other School Policies

The following policies should be read in conjunction with the E- Safety Policy

Policy	Date ratified
Safeguarding and Child Protection Policy	November 2018
Preventing Extremism and Radicalisation Policy	January 2019
Spiritual, Moral, Social and Cultural (SMSC) Policy	January 2019
Promoting British Values Policy	January 2019
Early Years Foundation Stage (EYFS) Policy	October 2016
Key Person Policy	October 2016
Relationship Policy	October 2018
Staff Code of Conduct and Behaviour Policy	October 2019
Supervision Policy	August 2018
Induction Policy	September 2019