



Stephenson Memorial Primary School

E-Safety Policy

Pending full Governing Body review
21/11/2016

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the ICT working group lead by the E-Learning Lead.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body	
The implementation of this e-safety policy will be monitored by the:	Head Teacher, E Learning Lead, ICT Technician, Class Teachers, Teaching Assistants.
Monitoring will take place at regular intervals:	ICT Technician (Weekly)
The Governing Body Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Governing Body Meetings
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2017

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
- Surveys / questionnaires of
 - students / pupils
 - parents / carers
 - staff

Scope of the Policy

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

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

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 Senior Leaders:

- 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.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-learning Lead other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders 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 support to those colleagues who take on important monitoring roles.

E-Learning Lead:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority and North Tyneside Learning Trust.
- liaises with school technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Technical Support:

The Technical Support is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety 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 / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies

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.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- they report any suspected misuse or problem to the Headteacher / Senior Leader / E-Learning Lead for investigation / action / sanction.
- all digital communications with students / pupils / parents / carers 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.
- students / pupils understand and follow the e-safety and acceptable use policies.
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection / Safeguarding Designated Person / Officer

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 on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school technology systems in accordance with the Student / Pupil Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's / academy's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / 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, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. 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, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety.
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events (eg LA / 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 / team meetings / INSET days.
- The E-Safety Co-ordinator / Headteacher will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / 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.

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 / academy 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.
- All users ([at KS2 and above](#)) will be provided with a username and secure password by Mr Duthie/Mrs Carr 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 every quarter.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- **Mr Duthie** 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. Content 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 has provided enhanced / differentiated user-level filtering
- School / academy technical staff 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 “guests” (eg 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 digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission .
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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:

	Staff & other Adults	Pupils
Communication Technologies		
Mobile phones may be brought to school	Locked away and only used in room or in the staff/PPA room. Staff permitted with mobile phones at all times: E Overton, C Garret, W Mitcheson, A Mason, R Hutton.	Phones to be handed into Office in the morning (Y6 only) and collected each evening.
Use of mobile phones in lessons	Not permitted	Not permitted
Use of mobile phones in social time	Staff room during break and lunch.	Not permitted
Use of other mobile devices eg I pads	iPads only.	iPads only.
Use of personal email addresses in school, or on school network	Not permitted	Not permitted
Use of school email for personal emails	Not permitted	Not permitted
Use of messaging apps	Not permitted	Not permitted
Use of social media Twitter, Google +	Twitter allowed	Not permitted
Use of blogs	Seesaw Blog	Seesaw Blog

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils 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 pupils, 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 pupils, parents / carers or school staff.
- They do not engage in online discussion on personal 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.

The school's use of social media for professional purposes will be checked regularly by the Headteacher and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 2015
- Prevent Duty Guidance 2015
- Working Together to Safeguard Children 2015
- How Social Media is Used to Encourage Travel to Syria and Iraq Briefing Note for Schools 2015

Non-statutory Guidance:

Promoting fundamental British Values as part of SMSC in schools:

- DfE Departmental advice for maintained schools 2014

Aims and Principles:

Stephenson Memorial Primary 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 pupils 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 pupils will know that the school has policies in place to keep pupils 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 pupils 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.

Pupils 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 pupils or staff will always be challenged and where appropriate dealt with in line with our Behaviour and Discipline Policy for pupils and the Code of Conduct 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 pupil's experiences and horizons.