Online and Safe Use Policy

Formally adopted by the Governing Body	**Nelson Infant School**
On:-	**12/09/2017**
Chair of Governors	**Sheila Wigg**
Last updated:-	**09/09/2017**

Contents

Appendix 7a/b – Letter to Parents reguarding Social Networking and follow up letter
Appendix 8 – Home/School Agreement Statement

Nelson Infant School Online and Safe Use Policy

1. **Introduction and Overview**

Rationale

Information and Communications Technology (ICT) is a central part of the curriculum as it plays an ever-increasing role in children's lives. On-line access is recognised as a means to support learning across the curriculum.

The purpose of this policy is to;

- Safeguard and protect the children and staff so that everyone can use the internet safely, and know that it is a positive resource to be treated respectfully.
- Set out the key principles expected of all members of staff at Nelson Infant School with respect to the use of technologies.
- Assist school staff working with children in order to work safely and responsibly with technologies, and to monitor their own standards and practice.
- Set clear expectations of behaviour relevant to responsible use of technologies for everyone at Nelson Infant School, albeit for educational, personal or recreational use.
- Outline clear procedures to deal with online issues.
- Ensure that all members of Nelson Infant School are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Who does this policy apply to?

This policy applies to all members of Nelson Infant School's community who support pupils and/or have access to and are users of technologies, both in and out of the School. This includes;

- **All** Staff (including teachers, TA's, one to one's, MSA's, cooks, cleaners, caretaker)
- Pupils
- Parents/carers
- Governors
- Volunteers
- Visitors/Other Users

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content

- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

How do we communicate this policy with our School Community?

This policy will be communicated to staff, pupils, and our school community in the following ways:

- Policy will be posted on the school website, in the staffroom, and a copy available in the school office.
- Policy is part of school induction pack for new staff, including information and guidance where appropriate.
- ICT Code of Conduct discussed with staff annually. (Appendix 1)
- All staff will have read and signed the ICT Code of Conduct before using any school technology resource. The office will keep a current record of this.
- The ICT Code of Conduct will also be shared with and signed by Governors, volunteers and other visitors.
- Regular updates and annual training on online safety for all staff, including any revisions to the policy.
- Pupil E-safety Rules (Appendix 2) shared regularly and a progressive E-safety Curriculum taught.
- Parents/Carers are asked to sign and return a consent form for Internet Use. The Pupil E-safety Rules will be part of this. The office will keep a current record of who is granted access.
- The policy is referenced in the Safeguarding policy, and in the school e-safety booklet which is given to each family at e-safety reading cafes, or when their child or children start the school.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead (DSL), acts as first point of contact for any safeguarding incident whether involving technologies or not.

- Any concern about staff misuse is always referred directly to the Headteacher/DSL, unless the concern is about the Headteacher/DSL in which case the concern is referred to the Deputy Head/Alternate DSL or Chair of Governors.

Review and Monitoring

This policy will referenced within other school policies (e.g. Safeguarding and Child Protection policy, Teaching and Learning, Computing policy).

- This policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to this policy will be disseminated appropriately to all staff and pupils.

2. Education and Curriculum

Using the Internet to Enhance Learning

Internet access for pupils at Nelson Infant School can be child led (both independent and supported) or planned to enrich and extend learning. Through a range or devices we want children to be able to access resources, research, communicate, and develop online skills in a safe and meaningful way.

Pupil Online Safety and the Curriculum

In Nelson Infant School we have a number of ways we encourage and facilitate safe use of the internet by the pupils, namely;

- clear, progressive e-safety Scheme of Work, as part of the Computing Curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- school developed E-safety Rules which are shared often with children, and are displayed throughout the school. All parents/carers have viewed these and signed their agreement to allow internet use at school. A home booklet includes these rules and how the school supports e-safety.
- designation by all children of responsible adults, both in and out of school, who support them when they need it (links to PATHs curriculum).
- development and use of passwords and usernames from Year 1 onwards.
- staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- the planning and implementing of an Internet Safety Day each year (Feb).

Staff and Governor training

This school;

- makes regular up to date training available to staff on Online Safety issues and the school's Online Safety education program. Governors will also be welcome to attend this training.
- provides, as part of the induction process, all staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct.

Parent/Carer awareness and training

This school:

- provides online safety information for parents/carers on the school website.
- requires each family to sign their support of the Nelson Infant School e-safety rules, and permission for their child/children to use the Internet (Appendix 3).
- provides a parent e-safety booklet which is given to each family when starting Nelson Infant School (available in the school office).
- has a yearly class Reading Café planned with an e-safety focus. The parent e-safety booklet will also be made available at this point.
- offers parents a yearly meeting to learn more about online safety, linked to staff training.
- will raise awareness through information/assembly following Internet Safety Day.
- will endeavour to review our practice and respond effectively to issues or concerns raised by parents/carers.

3. Incident Management

In this school:

- there is strict monitoring and application of the Online Safety Policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions (Procedures for Online Issues - Appendix 4)
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- All incidents should be recorded by a staff member on an E-safety Incident Report Form, available on the Server (ICT, E-safety), within this policy, (Appendix 5) or from the DSL. Action taken should be taken by, or overseen by the DSL. The Computing Subject Leader will be informed of any incidents which has arisen. Any incident forms will be stored in a secure file by the DSL.
- pupils and all staff are aware of the course of action for inappropriate sites.

- parents/carers are specifically informed of online safety incidents involving the children for whom they are responsible.
- support is actively sought from other agencies as needed (e.g. the Local Authority, ChildLine, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues. Phone numbers can be found on the Procedure for Online Issues document. (Appendix 4)
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- we will immediately refer any suspected illegal material to the appropriate authorities – e.g. Police, Internet Watch Foundation and inform the LA.
- complaints of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures.

Course of action for inappropriate sites on the Internet

- If pupils or staff discover unsuitable sites, the computer must be switched off at the monitor immediately. IPads will be returned to home page.
- Staff member responsible will complete E-safety Incident Form.
- The address (URL) and content must be reported to the Internet Service provider via the DSL/Headteacher, who will make ICT Subject Leader aware.
- Parents/Carers of the pupil(s) involved will be informed of inappropriate use of the Internet, whether intentional or not, by DSL or class teacher upon request of DSL.
- In the event of certain material being viewed or published, the police or local authority may be involved.

4. Managing IT and Communication Systems

Internet access, security and filtering

In this school:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision. Our broadband provision is currently with Norfolk County provider, Updata, and their linked Netsweeper internet filtering platform (July 2016 onwards).
- any adjustments made to the Netsweeper filtering platform will be discussed with ICT Subject Leader and made by the IT technician or ICT Subject Leader.
- any unsuitable on-line materials must be reported to a trusted adult (pupils) or ICT Subject Leader/DSL (staff).
- we have fortnightly visits from an IT technician through our contract with ICT Shared Services. This ensures that we have high quality support and management of our systems within school. Issues which need urgent attention outside these visits are supported by the contract.
- all school devices are linked to the network by Active Directory, which ensures only authorised devices are connected.
- the Identification Key is only known to our IT technician (ICT Shared Services), DSL/Headteacher and ICT Subject Leader, and is not released for personal devices or use.

- guest access of our wireless network is to be arranged with ICT Subject Leader or IT technician.
- Supply staff have a separate user account to access the school network via teacher laptops. Any documents for use by someone other than the person(s) a school laptop is allocated to, will be placed in a separate folder on the Server, called Supply folder.
- all changes to hardware and software can only take place through our Administrator account. This is managed by the IT technician, in discussions with ICT Subject Leader and staff.
- antivirus/malware checks take place regularly (upon each IT technician visit) and any issues are dealt with. Our support contract ensures that we have continuous cover.
- an Event Log on the Server attends to all errors and risks, and this is checked on each visit by our IT technician.
- discussions take place between the ICT Subject Leader and IT support regarding upgrades within the network. The school buys into the Refresh programme to cover costs.
- Local backups of essential school data are taken daily and stored securely off-site. Critical information is also backed up online.
- Staff are reminded termly about regular password changes and the need for strong, complex passwords. This concept is introduced to children in school in Year 1 when they each take ownership of creating their own.
- Staff are responsible for what happens on their login and should protect themselves accordingly ie log out, have short time automatic log outs on their laptops etc.
- Up to date training for the School Administrator is undertaken 3 times per year in order to maintain the Finance RAG Rating.

Email

This school;

- Provides staff with an email account for their professional use, ie. nsix.org.uk and makes clear personal emails should be through a separate account.
- We use anonymous e-mail addresses, for example head@, office@
- Expects anyone who has received an offensive email to speak to either their trusted adult (for pupils) or the DSL (for staff). The DSL will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.

Pupils email (when appropriate):

- We use school provisioned pupil email accounts that can be audited.
- Pupils are taught about online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use their nsix.org.uk email address for professional purposes.
- Access in school to external personal email accounts may be blocked.

- Staff will never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data /file must be protected with security encryption.

School website

- The school web site complies with statutory DfE requirements.
- Most material is the school's own work. Where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs of pupils or work published on the web do not have full names attached. Parents/Carers are required to sign a permission form (Appendix 6).
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- Within our school, 4 members of staff are able to edit the website, (Headteacher, ICT Subject Leader, School administrator and office assistant) and they are responsible for the passwords and usernames.
- The Headteacher has overall editorial responsibility and will ensure content is accurate and appropriate.

Social networking

All Staff and Volunteers;

- Will ensure that they 'establish safe and responsible online behaviours'.
- Are instructed to always keep professional and private communication separate, and consider raising their security settings where possible.
- There is an expectation that staff behave in an appropriate manner (as outlined in ICT Code of Conduct), in line with their professional standards.
- Will inform the Headteacher/DSL of any social contact with parents or carers.

Pupils:

- are taught about social networking, acceptable online behaviour and how to report any issues through our E-safety curriculum work.
- have developed and shared our age appropriate Pupil E-safety Rules. Parents/Carers have shared these with their child and signed an Internet Use Permission Letter.

Parents/Carers:

- Have the opportunity to attend a yearly meeting about e-safety which will remind parents about social networking risks.
- Receive communication from the school reminding them of acceptable behaviour in social media, and our school's procedures for online issues. This will take the form of a letter (Appendix 7a and 7b), a General Home/School Agreement including a social networking statement which is signed (Appendix 8), and additional communications, when required.

Personal Devices;

- Mobile phones will not be used during lessons, formal school time or when responsible for children, unless when there is an emergency or no other alternative.
- There is a school mobile available for the caretaker and swimming teachers which must be used in line with the ICT Code of Conduct.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).
- Parents or Carers who wish to share photos or videos of their child with school staff will be asked to email them to the office to be passed on to the appropriate staff member.

5. Data Security
Management Information System access and data transfer

In this school;

- We use Pupil Transfer or Common Transfer Files on Sims to create a file for the communication or transfer of sensitive data. This is a very secure system, accessed through a DfE secure site, which changes passwords regularly. The School Administrator is the only person who creates, transfers and receives these files.
- For the transferal of information within Norfolk, information can be shared through Any Comms+, or Norfolk County Council's Secure File Transfer Site.
- Sensitive information may also be sent to the school via encrypted e-mails.
- Sensitive information is stored securely.

6. Digital Content

Digital Images and Video

In this school:

- Photos and videos will only be taken on school devices and deleted as soon as they have been used.
- Photos and videos will be stored securely. This may be in lockable cupboards, or on the school network.
- We gain parent/carer permission for use of digital photographs or video involving their child/children. This consent expires one year after the child leaves school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- If we use photographs of individual pupils or small groups of pupils, we will avoid using the full name of that child in the accompanying text or photo caption.
- If we use photographs of individual pupils on our website or in publicity documents, we will not use the name of that child in the accompanying text or photo caption.
- Staff sign the school's ICT Code of Conduct and this includes a clause on the use of personal mobile phones/personal equipment.

- Individual parent/carer permission will be sought for photos used in other high profile publications e.g. newspaper.
- On School trips, photographs will only be taken on school cameras and for school purposes.
- In School Performances, Parents/Carers are asked to put away any mobile devices while pupils are performing. After the performance they can take photos of their child, when any children without permission given have been removed.
- At Sports Day, Parents and Carers are informed in writing prior to the event that photographs may be taken of their child for personal use only and that the privacy of other children and teachers must be respected at all times.

Writing and reviewing the Online Safety policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- The school has identified a member of staff who has an overview of Online Safety. In Nelson Infant School this is also our Designated Safeguarding Lead (DSL) and Headteacher, Rachel Barker.

- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.

STATUTORY FRAMEWORK

This policy has been devised in accordance with the following legislation and guidance:

- '*Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children*', DfE (2013)
- *Keeping Children Safe in Education'*, DfE (2014)
- Norfolk Safeguarding Children Board procedures
- Norfolk Safeguarding Children Board Protocol : Allegations Against Persons who Work with Children
- Guidance for Safer Working Practices for Adults who work with Children and Young People in Education Settings, DCSF, March 2009.