NAFFERTON PRIMARY SCHOOL

School e-Safety Policy

Why is Internet use important?

The internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes. Children and young people will experiment online, to enable them to take advantage of the many educational and social benefits of new technologies learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

- Children and young people use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students/children and young people who show a responsible and mature approach to its use.
- The purpose of Internet use in Nafferton is to raise educational standards, to promote pupil/children and young people's achievement, to support the professional work of staff and to enhance the Nafferton's management functions.

How does Internet use benefit children?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

Benefits of using the Internet include:

- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- exchange of curriculum and administration data with HCC and DfE;
- access to learning wherever and whenever convenient.

How can we ensure Internet use enhances learning and life experiences?

Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material will be taught.

- Internet access will be designed to enhance and extend education.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Nafferton School will ensure that the copying and subsequent use of Internet derived materials by staff, children complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of children.
- Staff will guide children to on-line activities that will support the learning outcomes planned for their age and maturity.
- Children and young people will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will children learn how to evaluate content?

Policies need to empower children and young people to evaluate content critically. Information received via the Internet, email or text message requires good information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. The extent to which the internet is used by extremists as a tool for radicalisation is not fully known , but it is clear that that persons responsible for recent attacks have accessed and been influenced by the internet to varying degrees. Extremist websites may be used to disseminate propaganda, spread news and updates on extremist issues, add radical interpretation to theological tracts and provision of discussion forums for like minded individuals. The internet also offers easily accessible downloadable extremist material including advice and guidance on bomb making, filtered out of public systems, but often not at home. policies need to empower children and young people to evaluate content critically.

- Children will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff, children and young people. Data security is a complex matter and cannot be dealt with fully in this document. We see data security as the responsibility of all staff maintain password security, care of equipment etc. Specifically the Head teacher, supported by the senior Leadership team, the IT coordinator and the IT technician take a lead in this area. Please report any problems to the head teacher. All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school.

Local Area Network (LAN) security issues include:

- Access to all ICT systems shall be via unique login and password. Any exceptions shall be recorded in the risk assessment and approved by the person in charge of data security.
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security.(The head teacher)
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the head teacher. This shall include the authorisation of access required by the ICT Support Team during investigations.
- Where ‘restricted’ information is stored, access shall only be granted to individuals approved by the head teacher. A record shall be kept of these approvals.
- All access controls will be reviewed each term, to ensure that any users that leave have their access removed. This is a standing item on the premises committee agenda
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations will be secured against user mistakes that compromise access or security and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed and must be password protected.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils’/staff work areas or attached to email.
- Files held on the organisation’s network will be regularly checked.
- The IT technician will review system capacity regularly.

How will filtering be managed?

Levels of Internet access and supervision will vary according to the child or young person’s age and experience. Access profiles must be appropriate for all members of the organisation.

- Nafferton School uses Quickline for broadband provision and they use Smoothwall for their filtering system.
- Requests for filtering changes from within the organisation will be made via (Mr Baird,Mrs Hammond, or Mr Saltonstall)
- The Head teacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children’s Social Care, IWF or CEOP. See Response to Risk Flowchart

How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and/or organisational use. The safest approach is to deny access until a risk assessment has been completed and safety established. Virtual online classrooms and communities widen the geographical boundaries of learning. The safety and effectiveness of virtual communities depends on users being trusted and identifiable. There are dangers for employees/volunteers however if personal phones are used to contact children and young people and therefore an organisationally owned phone should be issued. Abusive messages should be dealt with under the organisation's behaviour and/or anti-bullying policies.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Staff will be issued with an organisation phone where contact with children and young people is required.
- The sending of abusive or inappropriate text, picture or video messages is forbidden.

How should personal data be protected?

The quantity and variety of data held on children and young people, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual's rights;
- Kept secure;
- Transferred only to other countries with suitable security measures.

Organisations will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

Password security

Members of staff/volunteers with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords.
These steps will include:

- Keeping their password secure from others.
- Using a different password for accessing organisational systems to that used for personal (non-organisational) purposes.
- Choosing a password that is difficult to guess, or difficult for others to obtain by watching them login.
- Adding numbers or special characters (e.g. !@£$%^) can help.

How will email be managed?

The implications of email use by children and young people needs to be thought through and appropriate safety measures put in place. Un-regulated email can provide routes to children and young people that bypass the traditional boundaries.

A central question is the degree of responsibility that can be delegated to individual children and young people, as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

The use of email identities such as john.smith@[school] generally needs to be avoided by children and young people, as revealing this information could potentially expose a child to identification by unsuitable people.

For primary schools, whole-class or project email addresses may be used.

- Children may only use approved email accounts.
- Children people must immediately tell an adult if they receive offensive email.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used for communication outside of the school.
- Schools/organisations may have a dedicated email for reporting well being and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team/Senior Manager.

How will published content be managed?

Excellent websites can inspire children and young people to publish work of a high standard. Websites can celebrate children and young people's work, promote Nafferton and publish resources for projects. Sensitive information about the school and children and young people could be found in a newsletter but the website is more widely available. Publication of information should be considered from a personal and school security viewpoint.

The sending of pupil details must be typed and encrypted and sent from the admin email address.

- The contact details on the website will be the school's name, address, email and telephone number. Employee/volunteer or children's personal information must not be published.
- Email addresses will be published carefully, to avoid being harvested for spam (e.g. consider replacing '@' with 'AT').
- The appointed senior leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with guidelines for publications including respect for intellectual property rights and copyright.

Can pupil images and work be published?

Although common in newspapers, the publishing of children names with their images is not acceptable.

Strategies include using relatively small images of groups of children and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the organisational activity. Personal photographs can be replaced with self-portraits or images of children and young people's work or of a team activity. Children in photographs should, of course, be appropriately clothed.

Images of children should not be published without the parent's or carer's written permission. Some organisations ask permission to publish images of work or appropriate personal photographs on entry, some once per year, others at the time of use.

Children also need to be taught the reasons for caution in publishing personal information and images online.

- Images that include children will be selected carefully and will not provide material that could be reused.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of children are electronically published. Parents are asked to sign a permission slip on entry to the school, staff should check for exclusions in their class.

How will social networking and personal publishing be managed?

Parents/carers and professionals need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

Children will be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All adults should be made aware of the potential risks of using social networking sites or personal publishing either professionally with children and young people or personally. They will be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. The internet and social networking sites may provide a virtual online community to which a young person may wish to belong and then may in turn become increasingly exposed to extremism. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

•Nafferton School will control access to social media and social networking sites.
• Children will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
• Children will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the child or young person or his/her location.
• Employee/volunteer official blogs or wikis will be password protected and run from the organisational website with approval from the Senior Leadership Team/Senior Manager.
• Employee/volunteer will be advised not to run social network spaces for children and young people's use on a personal basis.
• Children will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children should be encouraged to invite known friends only and deny access to others by making profiles private.
• Children are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
Facebook is the main social media site that children are exposed to out of school and whilst the children at nafferton school are too young to use the site the year six teacher will talk about issues as they arise and as they are appropriate.

How will Internet access be authorised?
The organisation should allocate Internet access for staff members/volunteers, children and young people on the basis of educational need. It will be made clear to staff who has Internet access and who has not. It will also be made clear to users when they have Internet access and when they have not.This is part of the Acceptable use policies.

In a primary school, where pupil usage should be fully supervised, all children and young people in a class could be authorised as a group.

Parental permission shall be required for Internet access in all cases — a task that may be best organised when children and young people's home details are checked and as new children and young people join.

- The organisation will maintain a current record of all staff/volunteers, children who are granted access to the organisation's electronic communications.
- All staff/volunteers must read and sign the organisation's policies regarding information security and the use of information technology before using the organisation's ICT resource. (Acceptable use policy)
- For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- The Acceptable Use Policy is discussed in classes as an age appropriate document.
- Parents/carers will be asked to sign and return a consent form for children and young people's access.
- Parents/carers will be informed that children and young people will be provided with supervised Internet access, but must comply with the AUP at all times.

How will risks be assessed?

E-security and e-safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of digital technology is completely risk free. Information security is critical, in both protecting the information held concerning staff/volunteers, children and young people, and in ensuring the reliability of ICT systems to support teaching and learning.

As a minimum, the risk assessment shall be updated and reviewed annually by the Senior Leadership Team/Senior Manager of the organisation and reported to the Governing Body/Trustee. It is recommended that a review should be conducted each term.

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The organisation will need to address the issue that it is not possible to completely remove the risk that children and young people might access unsuitable materials via the system. It is wise to include a disclaimer, an example of which is given below.

- Nafferton School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither Nafferton School nor ERYC can accept liability for the material accessed, or any consequences resulting from Internet use.
- Nafferton School will audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will complaints be handled?
Parents and staff should know how to use the organisation's complaints procedure. If an issue arises alert the class teacher/head teacher who will then initiate the appropriate procedure.

How will Cyberbullying be managed?
Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF 2007).
It is essential that children, young people, organisations, and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

• Cyberbullying (along with all forms of bullying) will not be tolerated at Nafferton Full details are set out in our policy on anti-bullying.

Response to an Incident of Concern
An important element of e-safeguarding is the ability to identify and deal with incidents of concern and related to the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school shall establish an incident reporting procedure and record reported incidents in an Incident Log.

The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Senior Leadership Team/Senior Manager within the organisation at a minimum frequency of once per term. Through this review process, where deemed appropriate, management shall update the risk assessment in light of new incidents. The Log and accompanying action plans should be reviewed annually by the Governing Body.

Organisations could usefully draw up a list of common incidents from the log. For example:

* Circumventing the network security system
* Accessing inappropriate material (definition should be in AUP)
* Installing unapproved software
* Using other people's accounts, email addresses or passwords
* Breaching copyright
* Uploading school material onto a social network or chat room
* Leaving school mobile devices unattended
* Not logging off when leaving a device
Child Exploitation and Online Protection (CEOP)

Children need to know how to block someone online and report them if they feel uncomfortable. It is important to realise that there are people other than the staff in your organisation who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support.
Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.

What should the communications plan contain?

Nafferton School shall include appropriate communications and/or training for all sectors of the organisation's community.

This should cover:

- Workforce training in understanding the rationale for all e-safeguarding procedures and the consequences of inappropriate practice.
- Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as photographs, videos and podcasts in terms of permission seeking, taking, storage and retention.
- A comprehensive and developmental e-safety curriculum for children and young people referenced in schemes of work and programmes of study in schools.
- The programme should include the responsible use of web and communication technologies both inside and outside school and risks related to cyberbullying.
- Regularly re-visiting of the AUP with staff and pupils.
- ICT non-teaching staff training related to how digital technology can enhance learning and teaching.
- The school will create working Acceptable Use Policies (AUPs) based on all the agreed procedures for e-security and e-safety and covering ICT usage by all sectors of the organisational community. This policy shall be subject to annual review by the governing body/Trustee.

Organisations like ChildNet, ThinkyouKnow, CEOP offer support for education and training materials.

How will the policy be introduced to children and young people?

The children and parent agreement will be sent out to all parents. The policy will be on the web site and reminders will be put in newsletters. Consideration must be given as to the curriculum place for teaching e–safety; it could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever children and young people are using the internet.

A useful checklist could include:

- Every child to be informed that network and Internet use will be monitored.
- Children and young people's instruction in responsible and safe use should precede Internet access.
- Safe and responsible use of the internet and technology is reinforced across the curriculum.
- Particular attention to be given where children and young people are considered to be vulnerable.
- Opportunities for confidential discussions and pastoral support to supplement the planned curriculum.

Useful e–safety curriculum resources and programmes include:

- ThinkUKnow: www.thinkuknow.co.uk

- Childnet: www.childnet.com

How will the policy be discussed with staff?

It is important that all staff/volunteers feel confident to use new technologies in teaching and the organisation's e–safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

Particular consideration must be given when staff are provided with devices by the organisation which may be accessed outside of the organisational network. Organisations must be clear about the safe and appropriate use of organisational provided equipment and rules about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of the organisation's information.

All staff within Nafferton School including administration, governors and volunteers shall be included in awareness raising and training. Induction of new staff/volunteers shall include a discussion of the organisation's e–safety Policy.

- The e–safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and children, the organisation will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Manger/ Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

How will parents' support be enlisted?

Internet use in children's homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents/carers are aware of the dangers, children and young people may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents/carers plan appropriate supervised use of the Internet at home and educate them on the risks. Parents/carers should also be advised to check if their child's use elsewhere in the community is covered by an appropriate use policy. One strategy is to help parents/carers to understand more about ICT — perhaps by running courses and parent awareness sessions.

- Parents'/carers' attention will be drawn to our e-safety Policy in newsletters, the brochure and on the Nafferton School's website as well as through the organisation's Child Protection Policy and Procedures.
- A partnership approach with parents/carers will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–safety at other attended events e.g. sports days.
- Parents/carers will be requested to sign an e–safety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents/carers on e–safety will be made available to parents/carers in a variety of formats.