Waddington All Saints Primary School

"If they have wings, why make them walk?"

WHOLE SCHOOL ESAFETY POLICY
October 2016

This policy should be followed with due regard to the requirements of the School's Equality and Diversity Policy, Lincolnshire acceptable usage policy, keeping children safe in education 2016, child protection policy and the computing policy.

1)What is e-safety?

The School's e-Safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.
E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The internet has become an integral part of our own and children's lives. A world has opened up which offers many positive opportunities.

Children start using computers from a very early age and are increasingly using the Internet more and more whether it is at home, in school, on their mobile phones or on a games console. With this in mind, Internet Safety and knowing how to help protect children and young people online is essential.

Just as we want to keep children safe in the real world, we will want to do the same in the virtual world. It is important that we understand enough about the Internet to keep children safe from harm but is equally important that we equip children with the skills they need to keep themselves safe so they can experience the Internet positively and responsibly.

2)The potential risks

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify; intervene in and escalate any incident where appropriate.
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

3)The benefits of using the Internet in education

- Availability of a vast range of free and subscription educational resources to enhance the learning experience of pupils, including iTunes and apps;
- Access to world-wide educational resources including museums and art galleries;

- Facilitation of educational and cultural exchanges between pupils world-wide;
- Access to resources to facilitate enhanced learning for pupils with special educational needs;
- Access to experts in many fields, for both pupils and staff;
- Facilitating staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations, colleagues and parents;

4) Safe internet use

Most Internet use in primary schools is safe, purposeful and beneficial to learners. There is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery. Risks are magnified by the upsurge in schools' Internet access. However, many teachers feel that there is a far greater problem in the amount of irrelevant, incomprehensible material typically yielded by Internet searches.

For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. A procedure should be agreed with all staff on what to do, and how to handle the situation with pupils.

We urge teachers to think very carefully about allowing primary pupils to use Internet wide search engines such as Google. If Google is to be used at all, you must make sure that strict filtering is applied. Image searches are especially risky. There **may** be no need for pupils to download them, as long as an adult downloads the images before the lessons and stores them in a shared folder. When planning in internet research time, teachers will assess the risk and provide clear instructions for the pupils to ensure that they are searching in the safest way possible.
For example:
Close or minimise the image or window immediately. Don't try to navigate away. If pupils saw the page, talk to them about what has happened, and reassure them. Later, investigate the history of visited sites and how the pupil got there.
In view of the risks, we advise that primary pupils are supervised at all times when using the Internet. All staff should be aware that networked computers are generally online at all times when a user is logged on.

5)Filters and monitoring
At All Saints the governors and SLT do all they reasonably can to limit children's exposure to the above risks from the school IT system. As part of this process, the governing body and SLT ensure that we have appropriate filters and monitoring systems in place. All communication through the internet for both children and adults is filtered via a fortigaurd box and through systems developed by our ICT consultancy service (Infotech Direct). We strive to ensure that these systems are the safest possible.

Whilst considering our responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, the governors and Headteacher consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

We will refer to the guidance 'The UK Safer Internet Centre' guidance as to what "appropriate" might look like:
• UK Safer Internet Centre: appropriate filtering and monitoring

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. At All Saints no pupils are permitted to bring in mobile phones or similar technology devices that provide internet access through 3G & 4G, therefore this will enable them not to access the internet through unauthorised access in school.
Whilst it is essential that the governors and Headteacher ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

6)Staff training

Governors and the Head teacher recognise the requirement for staff to undergo regularly updated safeguarding training and that e-safety is part of this training. As part of our curriculum we ensure that we fulfil the requirement that children are taught about safeguarding, including online, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach (LCSB 5 year pathway).

7)Responsibilities

At All Saints we believe that the role of e-safety is a collective responsibility, to ensure the safety of our pupils.

7.1)Responsibilities of staff

- To ensure that they subscribe to the values and methods of the e-safety policy and apply this into their day to day practise in school.
- To always show discretion and professional conduct.
- To read and sign the **'Acceptable Usage Policy'** and apply this in their day to day practise.
- To notify the DSL of any incidents relating to e-safety.
- To report any breaches of the 'Acceptable Usage Policy' to the Head teacher.
- To engage with staff training in safe and responsible internet use as and when required.
- To ensure that an aspect of e-safety is taught termly (see computing curriculum overview) and that it is implemented through day to day practise in the classroom.
- Staff must not access or attempt to access any internet sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Senior Management Team so that it can be logged.
- Staff must ensure that access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.
- **Social networking** - should be blocked in all schools unless it is deemed educationally beneficial, at the discretion of the Headteacher. Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available.
- Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat.
- **Use of Email** - All members of staff should use their professional email address for conducting school business. Use of school email for personal/social use is at the discretion of the Headteacher.
- **Passwords** - Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.
- **Data Protection** - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced.
- **Personal Use** - Staff are not permitted to use ICT equipment for personal use unless school policy allows otherwise. If personal use is permitted, the school should emphasise what is considered within the boundaries of acceptance.
- **Images and Videos** - Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent.
- **Use of Personal ICT** - use of personal ICT equipment is at the discretion of the school. Any such use should be stringently checked for up to date anti-virus and malware checkers.
  Staff should note that internet and email may be subject to monitoring

7.2)Responsibilities of pupils

- To ensure that they always use the internet safely and to also remind others to do so.
- To learn how to use the internet safely and responsibly through the computing curriculum.

- To follow the school's e-safety rules at all times.
- To understand and sign a class **'Acceptable Usage Policy'**.
- To report anything that they are unhappy about in relation to the use of internet- in or out of school.
- To not bring any mobile phones or similar devices into school.
- **Use of the Internet** - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know.
- **Logins and Passwords** - every person has a different computer login and password. You should never allow anyone else to use your details. If you think someone else may have your details you should have your password changed.
- **User Areas** - your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home.
- **Security** - you should never try to bypass any of the security in place, this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.
- **Copyright** - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Please note that internet and email use may be subject to monitoring.

7.3)Responsibilities of parents

- To work in partnership with the school in teaching their child to use the internet safely.
- Acknowledge and read the **'Acceptable Usage Policy'**.
- Engage in e-safety support as and when required (workshops/ e-safety tab on the website).
- Encourage safe internet use at home.
- To speak to the school if they have any concerns in relation to use of the internet.

8) Security

8.1) Securing Information

The capacity of the school ICT systems and its security will be reviewed regularly. Security strategies, for the safeguarding of information, will be discussed and reviewed periodically with the service provider. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Personal data will be deleted when a pupil or member of staff leaves. Where possible photographs of pupils will only be taken using school equipment. In the age of the school rich social media presence and expectations of communication, personal cameras and mobile phones may be used but all images should be deleted once they have been uploaded to the school server or approved website.

8.2) ICT Security

- Virus protection will be installed and updated regularly.
- The school ICT systems will be reviewed regularly and the security of equipment, and their users, ensured.
- Security strategies will be discussed with our service provider and key messages from external sources will be used to influence decision.
- Administrative data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable/dmg files will not be allowed in pupils' work areas or attached to e-mail.

- Files held on the school's network will be regularly checked. The staff area of the G:drive will be swept and old files deleted appropriately.
- The ICT co-ordinator will ensure that the system has the capacity to take increased traffic caused by Internet use/increased file sharing.

8.3) Internet Dangers and Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The ICT coordinator will oversee Internet dangers, risk assessment and matters arising from Internet use.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

9) Communication Technologies

9.1) E-mail

Staff and pupils may only use approved e-mail accounts on the school system. Pupils must have adult supervision whilst using E-mail. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone without specific permission. E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

9.2) Social networking and personal publishing

The school will block/filter access to social networking sites. Social networking sites are not to be accessed by any pupil or member of staff at any time whilst using the school's ISP.
Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents will be advised of the dangers of social networking and steps will be taken to ensure that the children know and understand the legal restrictions of certain social networking sites. E-Safety awareness activities will be delivered regularly and involve pupils, parents and staff as appropriate.

10) Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed. Pupil mobile phones must not be used in school. The sending of abusive or inappropriate text messages is forbidden. No streaming between personal iPhones/iPads and school iPads should be established. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. ·
The ICT co-ordinator will ensure that the E-safety policy is implemented and compliance with the policy monitored.

11) The School Website

The point of contact on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. Website photographs will only be published with parental permission. Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.

12) School Twitter Accounts

All Saints Staff will be responsible for managing their Twitter account. Account details must follow the specified format and so that they can be identified as staff of All Saints. If a member of staff leaves, their Twitter account will be closed so that the new member of staff can set-up a new Twitter account using similar credentials. All Saints Staff Twitter accounts will only follow other All Saints Twitter accounts and educationally benefiting accounts-such as authors. Class Twitter accounts may be followed by individuals and groups outside school but

followers will be vetted regularly and deleted if deemed inappropriate. Children will not be mentioned by name and only photographs of children with permission will be used. No personal information will be shared.

Staff guidelines for tweeting:
-Use twitter as a general communication tool to capture all of the amazing learning that is happening in your class.
-Include a range of tweets (including groups working, learning outcomes, just a comment)
-Ensure a balance of children (not the same groups of children repetitively and no individuals)
-Only children who have given permission for their images to be used.
-No names or personal information to be used.
-Vet followers regularly and actively block anyone you deem to be inappropriate.

Leadership Twitter accounts will re-tweet top learning, only children with permission for photographs will be tweeted and no personal information will be used. Twitter will be used to collaborate with other schools to share ideas and celebrate success; it will act as a central hub for all of the amazing learning taking place. This will be streamed on the school website. Leadership will be vigilant in blocking inappropriate/offensive accounts and will check followers regularly.

Twitter is a tool school will use to communicate with parents. We feel it is important that children are aware of on-line technologies and are taught about how to be safe online; however no child at this school should be on twitter as the minimum age is 13. It is our duty to ensure online safety of our pupils; therefore if a child under the acceptable age use limit for Twitter becomes known to a member of staff, the member of staff will not interact with the child on this platform but will immediately inform the child's parents/carers. Children's accounts are not allowed to be accepted.

13) Curriculum
Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.
Each year group is taught an aspect of e-safety each term, the focus for this learning is: conduct, contact and content. (See computing curriculum overview for more information).

For example: If the aim is to teach search skills, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase.

Primary school learners need not be exposed to the risks of the unfenced Internet!

14)E-safety for pupils with additional needs
There is an underlying assumption that children have both understanding and application of "safety". Pupils need to understand that rules given to them must be followed. Pupils need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Pupils need to understand that certain rules will change and develop as they get older. Pupils need to learn how to apply strategies that will help them to avoid certain "risks" such that they need to plan ahead.

There are certain aspects of the above that are particularly challenging for pupils with additional needs and children who we may consider to be vulnerable in this learning context. Pupils will clearly have individual needs that will present a range of issues when teaching e-safety but some common difficulties may be:

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger children
- They are likely to find it hard to apply the same rules in different situations
- Most safety principles rely on children being able to explain what happened or to ask for help
- Some children may have poor recall and difficulties with learning through experience.

It would seem to be relevant for all schools to consider their e-safety policy in relation to specific adaptations that may be required for this group of pupils. It may also be helpful for SENCOs to coordinate advice between ICT specialists and support staff. This may take the form of child-focused strategies that would apply to a pupil with specific needs and would be made available to all staff involved in Internet use with that child.

12) Complaints

Responsibility for handling Internet misuse incidents will be taken by the ICT coordinator, initially. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure (see separate policy). Parents and pupils will need to work in partnership with staff to resolve issues. There may be occasions when discussions will be held with outside agency support to establish procedures for handling potentially illegal issues.

Useful websites:

CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website.
www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.
www.iwf.org.uk

Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same.
www.digizen.org