

THE SPALDING SPECIAL SCHOOLS FEDERATION

**ACCEPTABLE USE
OF ICT/
THE INTERNET/
E-SAFETY
POLICY**

Acceptable use of the Internet policy for SSSF

Contents:

1. Introduction
2. School Policy
3. School Procedures
4. Staff rules for responsible internet use
5. Parent Permission letter
6. Pupil Guidelines
7. Interactive whiteboard projector safety

1. Introduction

E - Safety Policy: February 2015

The Acceptable Use of the Internet and related Technologies

The aims of this policy and associated documents is to ensure the following areas are addressed in a manner that protects and guides all 'Stakeholders' in the use of Internet based technologies;-

- Managing the Internet safely
- Managing e-mail safely
- Using digital images and video safely
- Using the school network, equipment and data safely
- Infringements and possible sanctions

Context

The Internet and related technologies are powerful tools, which open up new prospects and opportunities for communication and collaboration.

The SSSF is embracing these new technologies as they bring with them a range of new approaches to education delivery for Teachers that will enhance our Children's education and promote our school within the local community.

“To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom.” DfES, eStrategy 2005

The **“Every Child Matters”** framework sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The ‘staying safe’ outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the ‘virtual world’ that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of our school to ensure that every child in our care is safe, and the same principles should apply to the ‘virtual’ or digital world as would be applied to our school’s physical buildings.

To help achieve this we will be using filtering/monitoring software called Capital Bytes solution. This filtering/monitoring software will also help us to educate our pupils in staying safe on the Internet.

THE SPALDING SPECIAL SCHOOLS FEDERATION

GENERAL INTERNET ACCESS POLICY

The computer network is owned by the Federation and made available to pupils to further their education and for staff to enhance their professional activities including teaching, research, administration and management. This Internet Access Policy has been drawn up to protect all parties – the pupils the staff and the school.

- The Federation reserves the right to examine or delete any files that may be held on its computer system or stand-alone machines and to monitor any Internet sites visited.
- Any breach of this policy, by staff or pupils, will result in the right to Internet access being withdrawn.
- All Internet activity should be appropriate to staff professional activity or the pupil's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT system, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Social networking sites are blocked at present in line with LCC policy.

Daran Bland

Headteacher

February 2015

2. Federation Policy

This Policy document is drawn up to protect all parties – our / your Children, our staff and our school. The aims of which are: - to provide clear advice and guidance on how to minimise the risks and how to deal with any infringements.

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of the Federation by children include:

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com, www.piczo.com, www.bebo.com, www.hi5.com)
- Video broadcasting sites (Popular: <http://www.youtube.com>)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, <http://www.miniclip.com/games/en/>, <http://www.runescape.com/>)
- Music download sites (Popular <http://www.apple.com/itunes/>, <http://www.napster.co.uk/>, <http://www.livewire.com/>)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements within the Federation:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive E-Safety education programme for pupils, staff and parents.

Reference: Becta - E-safety Developing whole-school policies to support effective practice

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in our school and our Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. Our Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to Mrs Cap (Computing coordinator, Priory) and Mrs Moore, (Garth).

Our e-Safety Coordinators they keep up to date with E-Safety issues and guidance through liaison with the Local Authority E-Safety Officer and through organisations such as the Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinators ensure our Headteacher, SMT and Governors are updated as necessary.

Our Governors have an overview understanding of E-Safety issues and strategies at our school and we ensure they are aware of our local and national guidance on E-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the Federations' Policy including the staff and pupil rules for responsible internet use to include:

- Safe use of e-mail;

- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data, to include the use of USB sticks
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about E-Safety matters at least once a year.

Staff will consult the Computing co-ordinators for advice on content, training and appropriate teaching levels consistent with the school's Computing programme of study.

Access to on-line resources will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Federation supports and respects each family's right to decide whether or not to apply for independent access.

Independent pupil use of telecommunications and electronic information resources is not advised and will only be permitted upon submission of permission and agreement forms by parents of pupils and by pupils themselves.

The school provides an E-Safety education programme for pupils, staff and parents. The Federation provides many opportunities for raising awareness concerning staying safe using ICT. Capital Bytes solution (filtering/monitoring software) will aid in the teaching of e-Safety and staying safe on the Internet. Both pupils and parents sign a computer usage agreement when pupils start the school (Priory). The Federation also holds staying safe curriculum days to heighten pupils' awareness. There are a number of displays and posters around school and the subject is integrated into schemes of work.

3. School Procedures

Resource Development

In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer "home pages" and menus of materials that are appropriate to the age range and ability of the group being taught. It is the responsibility of **all** curriculum coordinators to ensure that the use of ICT is included in all curriculum policies and to keep up to date with developments of ICT relevant to their particular curriculum area(s).

All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

Pupils may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

School Rules

The Federation has developed a set of guidelines for internet use by staff and pupils.

The rules for staff use, given on the next page, must be read and adhered to by all staff. Any breach of these rules may lead to disciplinary procedures.

All members of staff are responsible for explaining the rules and their implications to pupils. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

How will complaints regarding e-Safety be handled?

The Federation will take all reasonable precautions to ensure E-Safety.

However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Our school in conjunction with Ark ICT Solutions Ltd monitors computer activity and use. This includes all types of text from word documents written to webpage's viewed, with infringements reported to the Headteacher, after which

Staff or pupil(s) concerned are given information about infringements in use and possible sanctions.

Sanctions available include:

- interview/counselling by tutor / E-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- Referral to LA / Police.

Our Computing coordinator/E-Safety Coordinators will act as first point of contact for any complaint.

Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with Federation / LA child protection procedures.

Our E-Safety Policy has been created using Becta guidance and has been agreed by the Senior Leadership Team (SLT) and approved by the Governing Body.

Implementation of the policy

The Computing co-ordinators will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

The Federation will manage implementation of this policy with the support and guidance of the Local Authority.

General

This policy and its intentions will always reflect the present and future needs of all stakeholders and to support this we are always open to suggestions for changes and alterations of and to any specific individual provision / requirement to ensure full access to all.

This policy will be kept under regular review by the Curriculum and Standards Committee of the SSSF Governing Body.

4. STAFF RULES FOR RESPONSIBLE INTERNET USE

The computer network is owned by the Federation and made available to pupils to further their education and for staff to enhance their professional activities including teaching, research, administration and management. This Internet Access Policy has been drawn up to protect all parties – the pupils the staff and the school.

- The Federation reserves the right to examine or delete any files that may be held on its computer system or stand-alone machines and to monitor any Internet sites visited.
- Any breach of this policy, by staff or pupils, will result in the right to Internet access being withdrawn.
- All Internet activity should be appropriate to staff professional activity or the pupil's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person. Due to differing access rights staff should not allow pupils access to their user areas.
- Activity that threatens the integrity of the school ICT system, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

5. Parents' information letter

Monday, 16 January 2017

Dear Parents,



SAFE USE OF THE INTERNET

As part of the school's computing programme we offer pupils supervised access to the Internet. Before being allowed to use the Internet, all pupils are taught our rules and procedures, which are designed to ensure safe use for all.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. As you will realise however, some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. Whilst our aim for Internet use is to further educational goals and objectives, pupils may try to find ways to access other materials as well. Our rules and procedures are designed to prevent this happening.

We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school wishes to work with parents and families in maintaining high standards of protection.

During school, teachers will guide pupils toward appropriate materials. Our access to the Internet is strictly controlled by an electronic "firewall".

Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, mobile phones, movies, radio and other potentially offensive media.

We would be grateful if you could read the enclosed guidance document. Please do not hesitate to contact me if you have any queries.

Yours sincerely

Daran Bland

Head teacher

A parent's guide to the internet

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com, www.piczo.com, www.bebo.com, www.hi5.com.)
- Video broadcasting sites (Popular: <http://www.youtube.com>)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, <http://www.miniclip.com/games/en/>, <http://www.runescape.com/>)
- Music download sites (Popular <http://www.apple.com/itunes/>, <http://www.napster.co.uk/>, <http://www-kazaa.com/>, <http://www-livewire.com/>)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

There are potential risks associated with the above technologies; such as stranger danger relating to social network and chat rooms and children being threatened and intimidated by cyberbullying on Mobile phones. Here are a list of useful websites to help keep you well informed and your child safe. They can also be accessed via links on our school web-site. www.thinkuknow.co.uk; www.ceop.gov.uk; www.childnet.com; www.getsafeonline.org; www.iwf.org.uk; www.lincolnshire.gov.uk/lscb; www.kidsmart.org.uk/; www.saferinternet.org.uk; www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety; www.esafety-adviser.com/newsletter/.

If you would like more information about e-safety please contact Mrs Cap (ICT coordinator) at the Priory or Mrs Moore at the Garth.

6. Pupil guidelines for computer use

Our school has lots of computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only use the system with my own login name and password.
- I will not use other people's login names or files.
- I will only use the computers for school work.
- I will not bring in USB sticks or other storage devices from outside school unless I have been given permission.
- I will always ask permission from a member of staff before I use the Internet.
- I will only e-mail people I know or who my teacher has approved.
- The messages I send by e-mail will be polite and sensible.
- I will not give my home address or telephone number to anyone on the Internet.
- I will not agree to meet anyone via the Internet.
- I will report any unpleasant material or messages sent to me through the Internet.
- I understand that the school may check my computer files and may monitor my computer use.
- I will always hand my mobile phone into the office if I bring it into school.

7. Interactive whiteboard projector safety

Use of interactive whiteboards with projectors is becoming increasingly common in schools. Certain precautions should be taken to avoid discomfort and possible damage to the eye. Training in the safe use of the equipment is essential.



Guidelines for Users of Computer Projectors

When using any form of data projector, the following guidelines should be adhered to.

- Never stare directly into the projector beam.
- Keep your back to the beam as much as possible, and avoid standing facing into the beam for more than a few seconds at a time (the use of a stick or laser pointer* is helpful in this regard).
- Always step *outside* the projector beam when turning to face the class for more than a few seconds.

Teachers should:

- ensure that pupils are always adequately supervised whilst the projector is operating, and have been trained to follow safe routines of projector use.

(For further information concerning interactive whiteboard projectors refer to <http://www.hse.gov.uk/radiation/nonionising/whiteboards.htm>.)

The following page contains information about the safe use of interactive whiteboards. This information is displayed next to every interactive whiteboard in school to remind staff, pupils and visitors.

Safe use of the interactive white board

Please follow the health and safety guidelines.

Teachers should ensure that the precautions listed below are followed:

- Blinds should be closed only when the projector is in use.
- Reduce the brightness of the beam to suit the light level in the room.
- Remember not to stare directly into the beam of the data projector.
- Avoid standing facing into the beam.
- Remember to keep your back to the data projector beam when using the interactive whiteboard.
- Use a stick or laser pointer to avoid the need to enter the beam.
- Remember to secure or cover any trailing cables.
- Pupils should be briefed on the above and closely supervised when the projector is being used, especially when asked to point out something on the screen.

Thank you for using the interactive white board safely.