Art 17: Every child has the right to reliable information from the mass media. In Sperrinview we protect pupils from materials that could harm them eg websites, social networking etc.

Art 23: All pupils in Sperrinview have the right to lead a full and decent life with dignity and independence and to play an active part in the community (RRS team 2015)

Art 28: Every pupil in Sperrinview has the right to an education which will be differentiated to meet their individual needs (RRS team 2015)

Policy for E-safety and Acceptable Use of the Internet and Digital Technologies

Sperrinview Special School

This policy is informed by DE guidance
(DE Circular 2007/01 Use of Internet and Digital Technologies in Schools)

January 2012

CONTENTS

Introduction
ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Sperrinview Special School, we understand the responsibility to educate our staff on E-safety issues, to enable them to remain both safe and legal when using the internet and related technologies in the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs laptops webcams digital video equipment etc); and technologies owned by staff but brought onto school premises (mobile phones cameras and portable media players etc).

Monitoring
All internet activity is logged by the school's internet provider (C2K). These logs are regularly checked. Logs may also be monitored by the ICT co-ordinators and the school principal using RM Tutor.

Breaches
A breach or suspected breach of policy by a school employee or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach by staff is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, by the Southern Education and Library Board.
Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting
Any security breaches or attempts and any unauthorised use or suspected misuse of ICT must be immediately reported.

Additionally, all lost or stolen equipment or data, virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to:
Miss P Jordan (Principal)

E-mail
The use of e-mail within school is an essential means of communication for staff.

- The school gives all staff their own e-mail account to use as a work-based tool. By using your own school e-mail account you are clearly identified as the originator of a message.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients all mail is filtered and logged. If necessary e-mail histories can be traced.
- The use of Hotmail, BT Internet, AOL or any other Internet web mail service for school business is not permitted.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal (non c2k e-mail addresses.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Staff must inform the ICT co-ordinators [Miss P Jordan and Mrs S Duffin] if they receive an offensive e-mail.
- However you access your c2k e-mail (whether directly, through web mail when away from school or on non-school hardware) all the school e-mail policies apply.

E-safety
This policy, supported by the school's acceptable use agreements for staff, governors and pupils is to protect the interests and safety of the whole school community. It is linked to the child protection policy and the school's code of conduct.

ICT and on-line resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the staff on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- Staff receive information relating to e-safety through the ICT team.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safe-guarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- Pupils/parents are aware of where to seek advice or help if they experience problems when using the internet and related technologies, ie, parent/carer, teacher, assistant, or an organisation such as Childline or CEOP.
- E-safety posters are prominently displayed throughout the school.
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to an ICT co-ordinator.
- Deliberate access to inappropriate materials by staff will lead to the incident, depending on the seriousness of the offence:
  - being investigated by the Principal/C2K/Southern Education and Library Board
  - possible immediate suspension
  - possibly leading to dismissal and involvement of police for very serious offences.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction as well as a potential risk to young and vulnerable people.

All Internet activity in Sperrinview Special School is monitored and logged by our school service provider C2K. The logs are randomly but regularly checked and can be explored further if required. School work-stations can also be monitored by the school Principal via RM Tutor. Whenever any inappropriate use is detected it will be followed up. In order to maximise safe internet access:

- Staff will pre view sites before use.
- Raw image searches are discouraged when working with pupils.
- Parents/carers will be asked to supervise any Internet based homework.
- All users must adhere to copyright in relation to software and on-line resources.
- Staff will not upload any school related information onto the internet, with the exception of the School Web managers (Paula Jordan and Shaunagh Duffin).
- The use of camera-phones to take photographs is strictly forbidden by staff, visitors and pupils.
- Written permission must be obtained from parents before photographs can be taken of pupils.
- Written permission must be obtained from parents/carers before a pupil's image can appear on the school website.
- Staff are not permitted to use mobile phones when they are working with pupils (with the exception of emergency calls and in those circumstances written in risk assessments).
- Keep all personal calls to break and lunchtimes.
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
- If staff discover an unsuitable site the screen should be switched off/closed and the incident reported immediately to an ICT co-ordinator.
- All staff must comply with the school's 'Acceptable User Policy for the Use of the Internet and Digital Technologies'.

Social Net-working Sites

It is important to recognise that there are issues regarding the appropriateness of some content and contact in relation to social net-working sites. Staff are therefore encouraged to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Images once on-line can never be removed.

- Access to social net-working sites using c2k computers is forbidden.
- Access to social net-working sites using personal mobile phones during working hours is not permitted.
- Staff should not discuss any school related business on social net-working sites.
- Images of pupils or the school environment are not permitted to be uploaded on to social net-working sites.
- Images of staff are not to be uploaded on to social net-working sites without the permission of the staff member/s involved.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken for:
    - use in the school setting
    - use for training purposes by related professionals
    - used in the school website
- Parents/carers are expected to sign a Home School agreement containing the following statement: 'We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community'
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information evenings
    - Newsletter items
    - School website

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network:

- Staff should use their own personal passwords to access computer-based services.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Only disclose your personal password to authorised ICT support staff (Paula Jordan or Shaunagh Duffin) when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

Safe Use of Images

Taking, publication and storage of images

Digital images are easy to capture, reproduce and publish and therefore, issue. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and considering the appropriateness.

- The school permits the appropriate taking of images by staff with school equipment only with the written consent of parents/carers and staff.
- Staff are not permitted to use personal digital equipment such as mobile phones and cameras, to record images of pupils this includes when on field trips. Images can only be taken on school cameras.
- Permission to use images of all staff who work at the school is sought on induction.
- On a pupil's entry to the school all parents/carers will be asked to give permission to use their child's work/photos in the following ways:
    - on the school website
    - in the school prospectus and other printed publications that the school may produce for promotional purposes
    - recorded/transmitted on a video or webcam
    - in display material that may be used in the school's communal areas
    - in display material that may be used in external areas, ie exhibition promoting the school

    - general media appearances, eg local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
    - for training purposes by related professionals
- This consent form is considered valid for the entire period that the pupil attends this school unless there is a change in the child's circumstances where consent could be an issue eg divorce or parents, custody or child protection issues, etc.
- Pupils' names will not be published alongside their image and vice-versa on-line.
- Teachers must check that permission has been given for their pupils' images to be taken or published before an event takes place and before adding images to the website.
- Images of children are only permitted to be stored on the school's C2K network or on authorised password protected external storage devices provided by the school.
- Pupils and staff are not permitted to use personal portable media for storage of images (eg USB sticks).
- Rights of access to this material is restricted to the Sperrinview staff team.

Video Conferencing and the use of Webcams

The introduction of video conferencing has offered valuable educational and social opportunities to connect with other schools. Webcams in school are only ever used for specific learning purposes and all images recorded and transmitted are the responsibility of the teacher using them:

- Written permission must be obtained from parents/carers if their children are to be involved in video conferences.
- All pupils are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Principal is sought prior to all video conferences.
- The school conferencing equipment is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.
- Misuse of the webcam by any member of the school community will result in sanctions (as detailed earlier).
- Teachers need to be aware that non-Sperrinview participants in conferences may not be police checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Safe Use of School ICT Equipment

(including Portable and Mobile ICT Equipment and Removable Media)

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- ICT equipment issued to staff is recorded and serial numbers form part of the school's inventory
- All ICT equipment is kept physically secure.
- It is imperative that you save your data on a frequent basis to the school's network drive.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, return all ICT equipment to Miss Jordan or Mrs Duffin. You must also provide details of all your system logons so that they can be disabled.

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable and Mobile ICT Equipment

This section covers such items as laptops and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data:

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on the school network and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades (approximately every six weeks).
- The installation of any applications or software packages must be authorised by the ICT support team fully licensed and only carried out by your ICT support.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, iPod and iPad devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and then risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways to ensure that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and device s for their own use during non-contact time with pupils.
- The school discourages members of staff contacting a parent/carer using their personal device.
- The school is not responsible for the loss damage or theft of any personal mobile device.
- The sending of inappropriate text messages between members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and PDA for off-site visits and trips, only these devices should be used.

Writing and Reviewing this Policy

Staff Involvement in Policy Creation

Staff have been involved in the making of the Policy for E-safety and Acceptable Use of the Internet and Digital Technologies through training sessions and on-going consultation.

Review Procedure
There will be an on-going opportunity for staff to discuss with the ICT co-ordinators any issue of e-safety that concerns them.

This policy will be reviewed every 24 months (or sooner in relation to advances in ICT or if breaches have been detected) and consideration given to the implications for future whole school development planning.

A sub-committee of the Board of Governors will monitor and evaluate the effectiveness of this policy as part of a timetabled, on-going process.

Current Legislation

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Racial and Religious Hatred Act 2006
It is a criminal offence to threaten people because of their faith or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of *"Children and Families: Safer from Sexual Crime"* document as part of their child protections packs.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1-3)
Regardless of an individual's motivation, the Act makes is a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text music sound film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt o use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17-29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (section 1)
It is an offence to take, permit to be taken, make, possess show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene article" is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga 19980029 en 1

The Freedom of Information Act 200
http://www.ico.gov.uk/for organisations/freedom of information guide.aspx

Signed:_____Date:_____

Appendix 1

Acceptable Use Agreement/E-Safety Rules (Staff and Governors)

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- ► I will only use the school's e-mail/internet/and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal.
- ► I will comply with the ICT system security and not disclose any passwords provided to me by the school or C2k.
- ► I will ensure that all electronic communications with staff are compatible with my professional role.
- ► I will not give out my own personal details such as mobile phone number and personal e-mail address to pupils.
- ► I have been advised not to give out my own personal details such as mobile phone number and personal e-mail address to parents/carers.
- ► I will only use the approved, secure C2k e-mail system for any school business.
- ► I will ensure that school personal data is kept secure and is used appropriately, whether in school taken off the school premises or accessed remotely. All personal or sensitive data taken off-site must be encrypted on a teacher laptop (provided by C2k or on an encrypted external drive provided by the school.
- ► I will not install any hardware or software without the permission of the ICT co-ordinator.
- ► I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ► Images of pupils and/or staff will only be taken stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member.
- ► I will support the school approach to on-line safety and not deliberately share or upload any images, video or text that could upset or offend any member of the school community.
- ► I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request to the Principal.
- ► I will respect copyright and intellectual property rights.
- ► I will ensure that my on-line activity, both in school and outside school will not bring Sperrinview School or my professional role into disrepute.
- ► I will support and promote the school's e-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies in the context of school.
- ► I understand the sanctions related to breaches of the above.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Full Name (Printed) _____

Signature _____

Date _____