GREENFIELDS SPECIALIST SCHOOL FOR COMMUNICATION

E-safety Policy Reviewed January 2017

All policies at GSSC are written to reflect Statutory Requirements or National Guidance and updated in accordance with this. There are times when the Government or Local Authority provide updates to policies that are outside of the policy review schedules. In such instances, an appendix will be added to policies to reflect these updates until the Governing Board can ratify these amended policies. These appendices will supersede previously issued Statutory Requirements or National Guidance.

r pupils and staff at GSSC are treated equally regardless of race, age, creed, gender religion or sexual ation.

Policy Written by/date:	Signed/Date: Chair or Vice Chair	Policy due for review:
Mike Tebbutt: September 2015		September 2016
Mike Tebbutt: January 2017		January 2018

This Policy is linked to the following School Policies and/or Procedures

Curriculum Policies	School Policies	School Business/Finance Policies
• Curriculum • SEN • English (incl Library) • Art • DT • Forest Schools • Humanities • Maths • P.E • PSHE • ICT/Computing • R.E • Collective Worship • Science • Sex and Relationship Education (SRE) • Careers • Post 16 (inc Consortium) • Communication • ASD • Music • School Council • Spiritual, Moral, Social and Cultural including promoting fundamental British Values • Teaching and Learning • Conductive Education	• Child Protection and Safeguarding • Inclusion Policy and SEN Info • SEN Report • Positive Intervention • Prospectus • Pupil Attendance • Anti—Bullying • Designated Teacher (LAC) • Exclusions Policy • Volunteers • Animal Visits • Educational Visits • Exams/Accreditation • Staff Dress Code • First Aid Health and Medications • Intimate Care • Manual Handling/Mobility • Initial Teacher Training • Planning, Preparation and Assessment • Continuing Professional Development • Teaching Assistants • Well-Being of Staff and Student • SEF • SDP • Bereavement • Use of Photography and Video • Acceptable Use • E-Safety • Non-Smoking/Electronic Cigarettes Policy • Complaints • Assessment, Recording and Reporting • Parental Involvement • Student Participation • Home School Agreement • Healthy Eating • Transition • Pupil Premium • Supporting pupils in school with medical conditions	• Data Protection • Confidentiality • Pay Policy • Register of Business interests of HT and Governors • Accessibility Plan • Charging • Freedom of Information • Publication Scheme • Staff Grievance • School Companies • School Income • Lettings • Code of Conduct for all Staff • Governor Allowances • Allegations of abuse against staff • Health and Safety • Retention of data • Recruitment and Selection Policy (Safer Recruitment) • Governing Board Succession Planning • Whistleblowers • Instrument of Government • Staff Discipline, Conduct and Grievance procedures • Equal Opportunity Policy • Equality Duty • Staffing Structure • Staff Attendance Planned • Staff Attendance Unplanned • Anti-Harassment • School Emergency Plan • Critical Incidents • Transport • Pool Safety and Procedures • Lone working • Capability Policy • Visiting speakers policy • Appraisal

All our pupils and staff at GSSC are treated equally regardless of race, age, creed, gender religion or sexual orientation.

GSSC

E-Safety Policy

Introduction

This *(revised)* policy was reviewed in January 2017 by the Assistant Head. It was approved and adopted by Governors ……. It will be monitored and reviewed annually as part of the school's monitoring cycle or sooner if required. This policy complies with the DCSF December 2009 'Guidance for safer working practices for adults working with children and young people in educational settings'.

Rationale

Information and Communications Technology (ICT) 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. For example the internet technologies available both inside and outside of the classroom include: Websites; E-mail and Instant Messaging; Chat Rooms and Social Networking; Video Broadcasting; Music Downloading; Gaming as well as other programs/functionality that is constantly being introduced.

It is important to note:

- 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.
- Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial.
- All schools have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment.
- Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them.
- Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff continue to be protected.

At GSSC**,** we understand the responsibility to educate our students on e-Safety issues; teaching them the appropriate behaviours to enable them to remain both safe and legal when using the internet and related technologies, in and beyond 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. This can make it more difficult for your school to use technology to benefit learners.

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.

Scope of Policy

Both this policy and the Acceptable Use Agreement (for all staff, governors, and volunteers/workplace students and GSSC students (signed by parents) – appendices i, ii and iii) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and

technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Teaching and Learning

Why the Internet and digital communications are important

The internet is an essential element in 21st century life for education, business and for social interaction. GSSC has a duty to provide students with quality internet access as a part of their learning experiences.

Use of the internet is a part of the statutory curriculum and a necessary tool for students and staff.

Internet use will enhance learning

The school internet access for student use will include network filtering appropriate to the age of the students. Students will be taught what Internet use is acceptable and what is not. The school will ensure that the use of Internet derived materials by students and staff complies with copyright law.

E-Safety Roles and Responsibilities

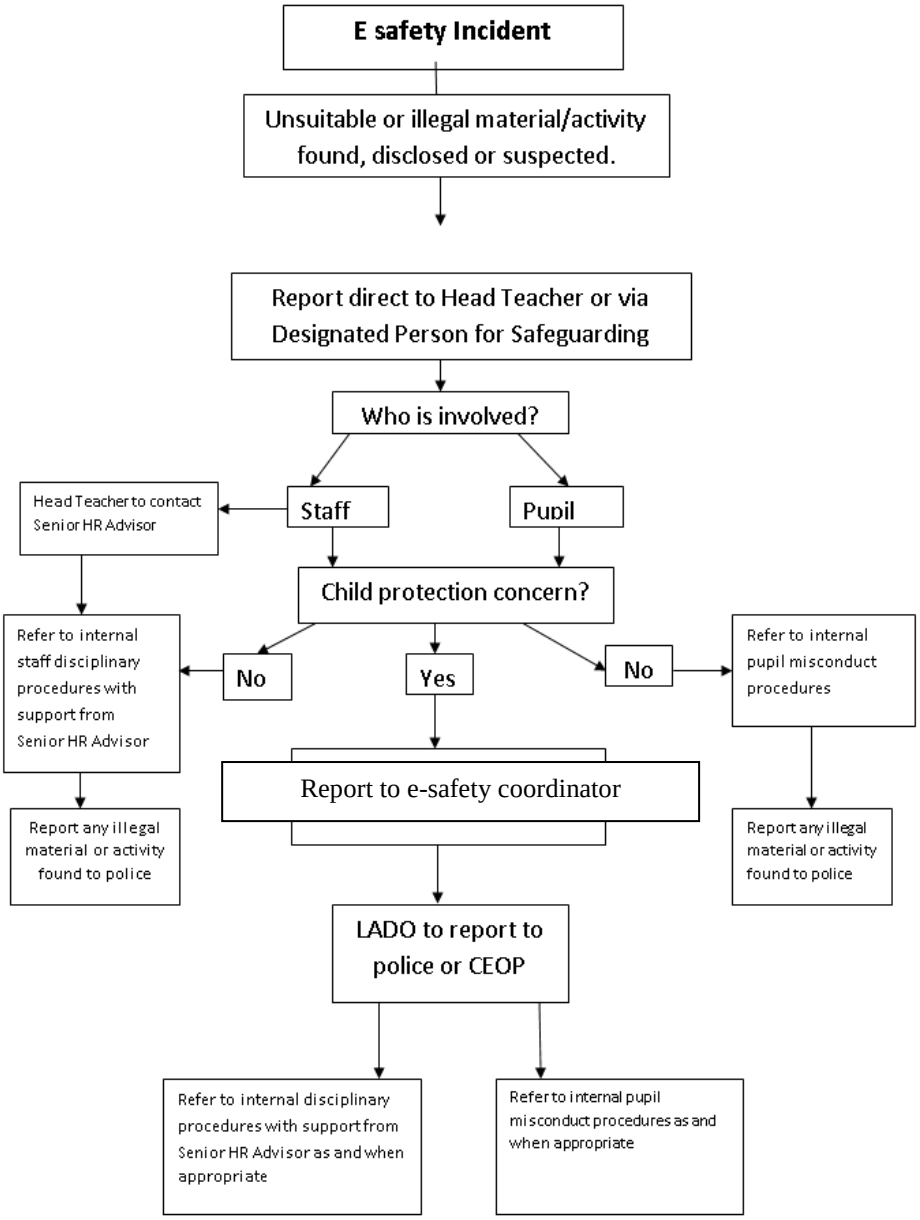
As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is Mike Tebbutt (Computing/ICT Coordinator). All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance.

Senior Management and Governors are updated by the Head/ e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.
This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to relevant school policies.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice.
ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm

or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.



ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All our pupils and staff at GSSC are treated equally regardless of race, age, creed, gender religion or sexual orientation.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Head Teacher/Designated Person for Safeguarding/e-Safety Coordinator immediately and recorded on the appropriate documentation (appendix iv) and the e-Safety incident flowchart followed. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the e-Safety coordinator.

Staff Responsibilities

Teaching and Support Staff (including Volunteers/Workplace Students)

All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound.

Please see Acceptable Use Policy for Staff, Governors, Volunteers/Workplace Students for further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email or related technologies within and beyond school. A copy of this document is made available to all staff and shared with any volunteers, visitors or workplace students.

Managing 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.

The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework (if appropriate to individual students), specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

➢ **Network Manager/Technical Staff**

Information System Security

The School ICT systems security will be reviewed regularly, to ensure appropriate controls are in place with regard to access. Virus protection will be updated regularly.

➢ If the school is using an outside contractor for technical services, it is the responsibility of the school to ensure that the managed service provider carries out

all of the safety measures that would be expected of the school's technical staff, including being provided with the School e Safety Policy and Staff AUP)

- The schools ICT set-up ensures:

- that the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- that anti-virus software is installed and maintained on all school machines and portable devices.
- that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the E-Safety Lead/ Designated Person for Safeguarding.
- that any problems or faults relating to filtering are reported to E-Safety Lead/ Designated Person for Safeguarding and to the broadband provider immediately and recorded on the e Safety Incident Log.
- that users may only access the school's network through a personal password
- that he/she keeps up to date with e safety technical information in order to maintain the security of the school network and safeguard children and young people.
- that the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E-Safety Lead/ Designated Person for Safeguarding.

Passwords and Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security

Users are provided with (if appropriate) an individual network, email, Learning Platform and Management Information System log-in username.

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, systems and/or Learning Platform. Individual staff users must also make sure that workstations are logged off after use.

E-Mail

Staff

- The school provides all Teaching Staff with a professional email account to use for all school related business, including communications with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Under no circumstances will staff members engage in any personal communications (i.e. via hotmail or yahoo accounts) with current or former students/parents outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform their line manager or the e Safety Lead if they receive an offensive or inappropriate email via the school system.
- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the e Safety Lead or Network Manager. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head Teacher

Students

- may only use approved e-mail accounts on the school system. In e-mail communication students must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- Staff and student information should not be published.
- Students are introduced to e-mail as part of the ICT Scheme of Work

Managing remote access

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school network and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Only equipment with the appropriate level of security should be using for remote access (i.e. encryption on any devices where sensitive data is stored or accessed)
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.

Internet Access and Age Appropriate Filtering

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content.

Safe Use of Images

Taking of Images

Digital photographs and videos are an important part of the learning experience for children and young people and, as such**,** schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and young people about the use of digital imagery within GSSC (see Video and Photography Policy).

- Written consent will be obtained from parents or carers before photographs or videos of young people will be taken or used within the school environment, including the school website or associated marketing material.
- Permission will be sought from any student or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Head Teacher for use of personal equipment for school related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device.

Publishing Student's Images and Work

GSSC seeks the consent of parents (on behalf of students) and staff, to use images and film for assessment and educational purposes including the inclusion of images on the school website and an up to date list is distributed to staff.

On entry to the school all parents/carers will be asked to give permission to use their child's/young person's work/photos in the following ways:
Photographs/videos:

N.B. Photographs and videos are used in school only as part of the home-school agreement.

a. Photographs/Videos to go home (to other Parents/Carers)
   YES / NO
   - This can be in another pupils Annual Review report or DVD as part of a group; on a communication device; as part as a residential DVD; in a photo taken in class; etc…

b. Photographs/Videos in the media
   YES / NO

Examples:

- For Education and Training purposes-other Professionals
- Greenfields School/LEA website
- Friends of Greenfields Facebook page
- For school media (e.g. newsletters; outside presentations)
- For external media (e.g. publication in the local press/websites/presentations – this may include social media)

Video conferencing
- Permission is obtained from parents and carers prior to their child's involvement in video conferencing.
- All pupils are supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities are time logged and dated with a list of participants.

Storage of Images
- Images/ films of students are stored on the school's network
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform

School ICT Equipment including Portable & Mobile ICT Equipment & 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
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory and that staff sign and accept the school's terms on issue of any equipment e.g. laptops

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all ICT equipment
- 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

Portable & Mobile ICT Equipment

This section covers such items as laptops, IPads, Tablets.

- Staff must ensure that all sensitive school data is stored on the network (shared drive) and not solely on the laptop or device, unless the device is encrypted. In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent fine. Password protection alone is not sufficient.
- Personal use of school laptops or computing facilities, whilst on site, is left to the discretion of the Head Teacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.
- Staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

Removable Media (Portable Hard Drive/Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. IEPs, pupil attainment and assessment data) off site, only encrypted memory sticks etc will be used.
- Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

Mobile Technologies

All our pupils and staff at GSSC are treated equally regardless of race, age, creed, gender religion or sexual orientation.

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, PDAs, gaming 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 the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use during non contact time with students. At other times these must be switched to silent.

- Students are not allowed to bring personal mobile devices/phones to school unless prior agreement has been sought from the Headteacher.

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.

- Personal mobile phones should never be used to contact children, young people or their families, nor should they be used to take videos or photographs of students. School issued devices only should be used in these situations.

- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher.

- The school is not responsible for the loss, damage or theft of any personal mobile device belonging to either staff or students.

School Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services
- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone.

<u>Current Legislation</u>

Acts Relating to Monitoring of Staff eMail
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 individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

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

Other Acts Relating to eSafety
Racial and Religious Hatred Act 2006
It 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 & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information www.teachernet.gov.uk
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 it a criminal offence to gain:
access to computer files or software without permission (for example using another persons password to access files)
unauthorised access, as above, in order to commit a further criminal act (such as fraud) impair the operation of a computer or program
UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

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 them 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 or 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 a 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.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Acceptable Use Agreement

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 are aware of their professional responsibilities when using any form of ICT. All staff, governors and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **Mike Tebbutt** School e-Safety coordinator/Computing Coordinator or
Terry Hollowell School Business Manager.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will ensure that personal data (such as data held on software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students 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. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds 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 Headteacher or Senior Leadership Team
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute and in particular through the use of 'social networking' sites.
- I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

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

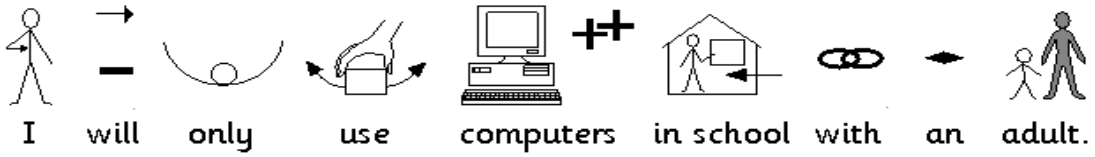
Signature …… Date ……

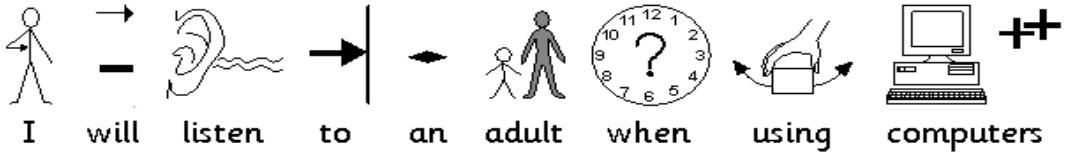
Full Name ……..……..... (printed)

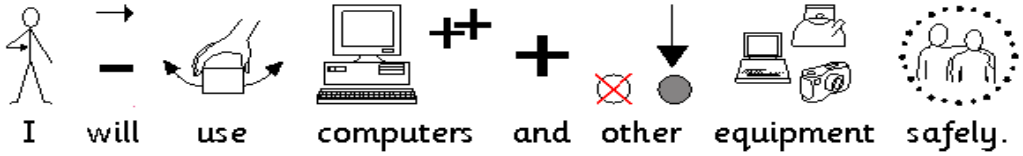
Job title or Role in School . . . . . .

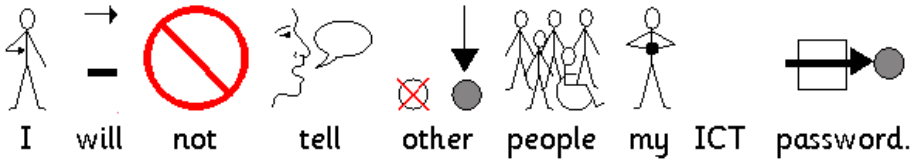
All our pupils and staff at GSSC are treated equally regardless of race, age, creed, gender religion or sexual orientation.

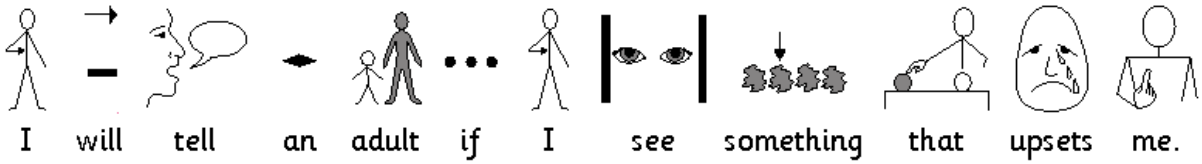
Using
Computers and the Internet Safely











All our pupils and staff at GSSC are treated equally regardless of race, age, creed, gender religion or sexual orientation.

Greenfields Specialist School for Communication
Prentice Court
Goldings
Northampton
NN3 8XS
01604 741960

Dear Parents/ Carers,

E-Safety

ICT including the internet, e-mail and mobile technologies, etc have become an important part of learning in our school. We expect all students to be and feel safe and with appropriate support, use these technologies responsibly within School.

Whilst we appreciate that all of our students are individuals and that not all statements will apply to all students, we are asking parents/carers to work with the school in order to continue to provide your child/young person with a safe learning environment. Please read and discuss (if appropriate), these e-Safety rules with your child/young person and return the slip below to confirm acknowledgement.
If you have any concerns or would like to discuss this further, please contact me at school.

Many thanks for your continued support and cooperation.

Mike Tebbutt
ICT Coordinator

✂ ----------

Parent/ carer signature

We have read the e-Safety rules and discussed (if appropriate) them with our child/young person ……..(name)

We agree to support the school in continuing to provide a safe learning environment for our child/young person and to support the safe use of ICT at GSSC.

Parent/Carer Signature ……

Class …… Date ……

GSSC
***E-Safety* Incident Log**

Details of ALL e-Safety incidents to be recorded by the e-Safety coordinator. This incident log will be monitored by the Headteacher, Member of SLT or Chair of Governors.

Date & time	Name of student or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons