E-Safety - Responsibilities of school staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-Safety issues with pupils. Further advice can be sought from Lincolnshire Safeguarding, or from CfBT ICT consultants.

The trust between pupils and school staff is essential to education but very occasionally it can break down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. Nationally, CEOP was set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders" and their work should be acknowledged and built upon by schools. Within Lincolnshire a member of staff who flouts security advice or uses ICT technology for inappropriate reasons risks dismissal.

All staff should sign an Acceptable Use Policy on appointment. Staff thereby accept that the school can monitor network and internet usage to help ensure staff and pupil safety.

Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. Procedures must define how inappropriate or illegal ICT use is reported to the Senior Leadership Team. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source.

Email, text messaging, Social Networking and Instant Messaging (IM) all provide additional channels of communication between staff and pupils. Inappropriate behaviour can occur and communications can be misinterpreted. Staff should be aware of the power of the Police to identify the sender of inappropriate messages. Schools should provide establishment email accounts for all staff.

Staff should be aware that students may be subject to cyberbullying via electronic methods of communication both in and out of schools. Head teachers should be aware that they have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site (Education and Inspections Act 2006)

School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy (Education and Inspections Act 2006).

Any allegation of inappropriate behaviour must be reported to the Senior Leadership Team and investigated with care.

If there is any suspicion of illegal activity staff should NEVER investigate themselves but must report to Lincolnshire Police as soon as possible.

E-Safety Policy (School Staff)

This policy has been created with a school emphasis using the e-safety policy of Lincolnshire Safeguarding Children's Board and the Acceptable Use of ICT Policy (AUP). This is a minimum requirement to which all school staff should adhere

Internet access
You must not access or attempt to access any 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 or access may be required for educational purposes only. For example, 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.

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 until such a time where students and staff have received sufficient education in the dangers and are able to safeguard themselves online.

If social networking is allowed ensure that there is strict policy with regards to security of personal details, rather than relying on the default settings. You should also ensure that any age restrictions are adhered to (many social networking sites have a minimum age of 13 years). 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.

Guidance on teachers using social networking sites e.g. Facebook[1]

This advice builds on the Safeguarding Policy that you can find in the Staff Handbook. It states that all adults working in our school have a duty of care to provide a safe, caring and supportive environment for all students to secure the well-being and very best outcomes for our students. We are confident that all staff in this school are fully committed to this policy and support the "Stay Safe" element of the ECM programme.

One area of the safeguarding agenda that is very high profile currently is e-safety. We need to take great care in the way we communicate electronically with students. The advice is that any electronic communication should be transparent e.g. using the school e-mail system, using the VLE from September 2010.
Staff should not share any personal information electronically with a student, nor should staff request/respond to any personal information from a child. This means that staff should not have current students listed as Friends on social networking sites such as Facebook. Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat.

It is appropriate in certain circumstances to share mobile phone numbers but this should always be for a specific purpose. Staff and students should delete those numbers once the purpose is finished e.g. staff always exchange mobile numbers on expeditions but delete numbers at the end of the expedition.

This advice might sound archaic however staff who share personal information with students using non-SGS communication systems without the agreement of SLT and parents are leaving themselves open to allegations of unprofessional conduct, or at worst to criminal investigations. This is a short section of the advice:

"Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming".

If you want further guidance on this please consult "Guidance for Safer Working Practice for Adults who work with Children and Young People" published by Lincs 2010 also available on www.dcsf.gov/everychildmatters/resources-and-practice/IG00311/ The Education version of that document includes this very clear advice:

This means that adults should:

- *Ensure that personal social networking sites are set at private and pupils are never listed as approved contacts.*
- *Never use or access social networking sites of pupils.*

[1] Memo from CML circulated to all staff July 2010

Use of Email
All members of staff should use their professional email address[2] 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.

File sharing
Technology such as peer to peer (P2P) and bit torrents[3] is not permitted on the Lincolnshire School's Network.

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.

Viruses and other malware
Any virus outbreaks are to be reported to the Mouchel Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

[2] name@spaldinggrammar.lincs.sch.uk

[3] BitTorrent is an open source peer-to-peer protocol for downloading files on the internet. Open source means the code is available for anyone to modify and redistribute at will. Consequently there are several free BitTorrent programs available to the public, each with differing features. The idea behind BitTorrent is to allow massive distribution of popular files.

Staff should note that all files stored on the school's hardware, internet usage and staff's use of school email may be subject to monitoring without prior notice.

E-Safety Policy (students)

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Pupils should note that all files stored on the school's hardware, internet usage and pupils' use of school email may be subject to monitoring without prior notice.

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. This would include pornography, discrimination, racial or religious hatred. 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. Never try to bypass the security by using proxy[4] sites, these are all monitored.

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. It is your responsibility to keep these details private.

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.

[4] A server that sits between a client application (e.g. a Web browser) and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes**:** Improve Performance & Filter Requests **(**SGS uses a proxy server to prevent pupils from accessing inappropriate websites).

Installing software
Under no circumstances are pupils allowed to install, download or upload their own software or programmes on to the school's system. Programme files (e.g. .EXE files must not be stored on the school's network)

Social Networking
Social networking (for example Bebo, Facebook, Flickr, Instagram, Snapchat) is not allowed at SGS but the following guidelines offer sound advice for pupils who use social networking sites outside of school;

- You should never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself, videos and pictures can easily be manipulated and used against you.
- You should never make negative remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc.
- Consider using a nickname and only inviting people you know.
- Universities and future employers have been known to search social networking sites. Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right follow your instincts and report it to an appropriate adult.
- Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.
- Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise.
- It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

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.

Etiquette
SGS provides pupils with email accounts and may let them post on things like blogs. Always be polite and don't swear. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones

Some modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. But, in the same way that some internet services can be used inappropriately, the same is true with mobile phones. If your school allows mobile phones in the classroom, these should not be used during the lesson unless your teacher has given you permission. Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act.

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

BBC - a fantastic resource of e-safety information for the younger child.
www.bbc.co.uk/cbbc/help/web/staysafe

Cybermentors is all about young people helping and supporting people online.
www.cybermentors.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

Some simple do's and don'ts for everybody (courtesy of CEOP):

- Never give out personal details to online friends that you don't know offline.
- Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family. Small pieces of information can easily be pieced together to form a comprehensive insight into your personal life and daily activities.
- Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.
- It can be easy to forget that the internet is not a private space, and as result sometimes people engage in risky behaviour online.
- Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent or carer to see.
- If you receive spam or junk email and texts, never believe the content, reply to them or use them.
- Don't open files that are from people you don't know. You won't know what they contain—it could be a virus, or worse - an inappropriate image or film.
- Understand that some people lie online and that therefore it's better to keep online mates online.
- Never meet up with any strangers without an adult that you trust.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

E-Safety Policy (recommended steps)

Here are some thoughts and recommended steps for all schools:

1. Technology - the two technology tools available to schools to provide assistance in safeguarding are internet filtering and Securus behaviour management.

Internet filtering - take some time to discuss with your technical team or your managed service provider which categories are blocked and which are allowed. Who makes the decision to block or unblock, the technical team or those delivering the curriculum? Are your staff and students being overly blocked through a "locked down" system or is the system being properly managed? Are there steps in place to have internet sites blocked or unblocked quickly? What do the students think, do they feel they are being overly blocked? Does your school run regular reports to see if there has been any inappropriate inactivity?

Securus behaviour management - this is a new tool which has recently become available to all schools for free (with a one-off training cost). It can help protect students from cyber bullying, grooming, racist and harmful behaviour. The software takes a screenshot of anything it believes may be inappropriate or illegal, based upon pre-defined rules and threshold levels. It then emails this screenshot to a selected person within the school. If your school has this installed, are both staff and students monitored? If you don't have it installed you should give it serious consideration.

2. Policies - the policies within this booklet are a minimum standard and take into account both e-safety and acceptable use. You are free to design your own policy and change to more suitable wording, as long as the context remains. Staff and students should all sign that they understand and accept the policies, and visibility of these policies should also be given to parents.

3. Training - are all staff aware of e-safety, not just teaching staff? Are the students aware? You must be aware of your duty of care as a school, and also your requirements under Ofsted. Are there safety training and awareness sessions available for staff, students and parents? If your school is not confident, consider contacting CfBT and using its accredited training sessions.

4. Guidance - technology moves at such a pace, and risk taking behaviours evolve into other risks. Ongoing training and guidance, particularly as part of CPD is a must. Have you signed up to the monthly e-Safety newsletter which will keep you up to date with other training initiatives?

5. Responsibility - this lies with the Headteacher and governing body. Are you aware of your responsibilities and duty of care? Has this responsibility been devolved to the technical team? If so, why? These are not technical issues but potentially very serious pastoral ones.

Spalding Grammar School – ICT User Agreement 2009

All software for students is available via the desktop to support ICT and curriculum based lessons. Students must not access the 'C' drive or the operating system of the PC, nor sabotage or interfere with the system or with any other pupil's work, including irregular or illegal activity (such as the possession or use of viruses, password breakers or similar files). Users may only use USB pen drives to transfer work from home, the memory stick must not contain any programs or other files that could be run on the school network. Anyone caught running unauthorised programs will be subject to the school disciplinary procedure.

E-MAIL

Because of the nature of the organisation, any e-mail or attachments are considered the property of the school and may be monitored, especially as the school acts in loco parentis. Any findings will remain confidential, but disciplinary action may be taken for inappropriate use of the system. This would include any students found to be deliberately sending offensive messages, 'spamming' the system or using other people's e-mail login names. Students must not open any e-mail where the content is suspicious nor open suspect attachments without speaking to the Network management staff.

INTERNET

Students are expected to use the Internet appropriately. They are encouraged and have the right to examine a broad range of information, opinions and ideas for the purpose of educational research. They have a responsibility to ensure their use is educational and ethical. Students should not communicate with strangers unless with the permission of staff and should avoid giving personal or financial details. It is unacceptable to access chat rooms or messaging services unless instructed by a member of staff; personal photos should not be sent without parental agreement; unacceptable websites should not be accessed; games simulations or software must not be downloaded; obscene, vulgar or inappropriate language or material must not be used or transmitted. Users should report misuse of the Internet to staff. Teachers and the school will determine what is appropriate material and use and shall not be held liable for any materials retrieved from the Internet by students.

I undertake to abide by the ICT User Agreement and I have read the above code of practice. I accept that the school is not liable for lost, damaged or unavailable information due to technical or other difficulties and is not responsible for what users do or the information they access. I acknowledge that the majority of such information is generated outside of school control.

I fully understand that if I do not abide by this ICT User Agreement, my access privileges may be withdrawn and that disciplinary or legal action may be taken against me. When unsure of any procedure or policy, I accept it is my responsibility to

ask a member of staff. I will not use other people's passwords nor communicate my passwords to anyone else.

I understand that all staff have the right to access my work on the school network at any time without prior warning.

Student Name: ……..

Student Signature: …….. Date : ……

Parent/Guardian:
As parent/guardian of the above student, who is under the age of 18, I understand all of the above and accept full responsibility for my son or daughter's actions.

Signature: …….. Date : ……..