Online Safety and Computer Usage Policy

1. Introduction

New technologies have become integral to daily life whether in or outside of schools. The internet and other digital and information technologies are powerful tools as both a means of communication and in facilitating extensive access to, and sharing of, information.[1] At Old Swinford Hospital we recognise and value the benefits this can bring to a student's education but are cognisant that these technologies can pose threats and risks not only to the user but also to others.

2. Guiding Principles

2.1. The School is committed to safeguarding and promoting the welfare of its students both within the school environment and outside whilst in the care of the School and this Policy intends to give direction as to how the School seeks to educate students to explore their horizons by using online devices and technologies and by doing so with safety, caution and responsibility for themselves and with respect for others.

2.2. Governors have overall responsibility for safeguarding and promoting student welfare and well-being at the School however protecting students and securing their welfare is also the responsibility of all staff. The School has a Safeguarding Policy in place and its procedures will be followed where there are any matters arising from the use of the internet or of electronic devices which compromise student safety and/or welfare.

2.3. This Policy applies:

2.3.1. To all members of the school community including students, staff, volunteers, parents[2] and visitors[3] when they are on site and at all times when they are using the School's network or devices whether on site or remotely.

2.3.2. To all students, staff and volunteers when they are off the school site for incidents which may take place out of school but are, or can be, linked to membership of the School.

2.4. The School will adhere to the principles of the Data Protection Act and other relevant legislation.

2.5. Complaints arising under this Policy will be dealt with under the School's Complaints Policy or, if appropriate, under the staff Grievance Procedure.

2.6. The following policies should be read in conjunction with this Policy:

- Behaviour Policy including the School Rules, Code of Conduct for Students, School Dress Code, Regulations for Registration, Absence and Leaving School Grounds, Rewards & Sanctions, Anti-Bullying, Drugs/Substance Use and Misuse, and Student Use of Electrical and Electronic Equipment & Internet Guidance
- Boarding Policy
- Code of Conduct for Staff & Volunteers
- Data Protection Policy
- Email and Internet Usage Policy

[1] For the purposes of this Policy any reference to the internet and or electronic devices (or these technologies in general) will include all access to technology based information or methods of communication including the use of the School's network and any of its devices (either linked or standalone), the use of own or third party devices for any form of internet access, means of communication or other associated use including but not limited to the use of 'Cloud ' based provision and any form of social media.

[2] Any reference to parents includes carers.

[3] Any reference to visitors includes contractors

- Information Security Policy
- Password Policy
- Publication Scheme on Information Available under the Freedom of Information Act
- Safeguarding Policy and Procedures

3. What the School will do

The Governors and the School have a set of clear expectations and responsibilities for all users and on behalf of the Governing Body the Headmaster will:

3.1. Maintain and implement a series of policies and procedures through which behaviour and actions can be moderated, risk may be assessed, controlled or mitigated and which will provide the means for acting and reporting on issues thereby securing the welfare of students including a Safeguarding Policy, Risk Assessment Policy, Behaviour Policy and Behaviour Management Policy.

3.2. Designate a member of staff to be the Online Safety Officer who may be delegated to act on any matters within this Policy as well as taking day to day responsibility for online safety issues.

3.3. For the purposes of this Policy the designated Online Safety Officer will be the Deputy Headmaster who is also the School's Designated Safeguarding Lead (DSL).

3.4. Ensure all staff are:

3.4.1. Aware of, and adhere to, the School's policies and procedures for the health, safety and welfare of students.

3.4.2. Appropriately trained in matters of online safety and are vigilant throughout the day and in boarding time for any signs of potential misuse or abuse of technology.

3.4.3. Aware of the regulations permitting and guiding the searching of electronic devices.

3.5. Provide adequate and suitable education and training for students, through the curriculum and in general, so that they can be better informed in the use of, and potential threats/risks associated with the use of, the internet and of electronic devices. Good educational provision should help students build resilience to the risks to which they may be exposed and have the confidence and skills to face and deal with these risks. Good educational provision should equally improve the students' skills and knowledge in the use of ICT facilities so that they can take advantage of the value of having access to such a vast amount of information, employ it discerningly and well in their learning and use ICT resources to produce informed and well-presented studies.

3.6. Engage with parents to ensure that they are equally informed of the potential threats/risks associated with the use of the internet and of electronic devices and gain their support in expecting their children to be safe users of technology both in and out of school.

3.7. Set boundaries for the use of the School's own network and devices, and for personal ICT equipment used in school, including the use of social media services.

3.8. Ensure there is a routine and regular monitoring system in operation within the School's own network and its internet provision.

3.9. Ensure that there is a clear and consistent approach for responding to incidents.

3.10. Liaise and share information about concerns with local and national agencies who need to know and involving students and their parents appropriately.

3.11. Appraise Governors, at least annually, of education and training initiatives undertaken, any identified risks and any incidents. Reporting should be more regular where incidents are serious or frequent.

4. Students and their Parents

4.1. Students are required to assume responsibility for their own behaviour and this extends to their use of the internet and any electronic devices. The School's Behaviour Policy makes it clear that:

4.1.1. Students should be respectful and tolerant of others and be mindful of, and responsible for, their own welfare and that of others.

4.1.2. Any form of bulling behaviour or harassment will not be tolerated.

4.1.3. Students should adhere to the Acceptable Use Agreement.

4.2. The School's Behaviour Policy includes a section on Student Use of Electrical and Electronic Equipment & Internet Guidance. This is issued to all new students and the prevailing copy housed thereafter on the School's website for future reference.

4.3. The rules applied to the use of the School's network and its devices apply equally to students' own internet, communications access and relevant devices.

4.4. Students must accept and adhere to the boundaries of use of the School's own network and devices, or personal electronic equipment used in school, including the use of social media services and mobile telephones.

4.5. The Education and Inspections Act 2006 permits the regulation of the behaviour of students when they are off the school site including the imposition of sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this Policy, which may take place out of school, but is linked to membership of the School.

4.6. Students should be aware of how they can report areas of concern whilst at school or outside of school and how, if they choose, they can use the School's anonymous reporting system.

4.7. Parental engagement is vital to ensure that students are as safe online at home as they are in school. Recognising the boarding nature of the School and therefore the distance between school and students' homes, parent information should be distributed by wider means than solely school based events. Parents should be encouraged to ask for information and guidance if they need it.

5. ICT Support, Security and Monitoring

5.1. The School's ICT Support both filters and monitors access to the internet.

5.1.1. Filtering should be sufficient to reduce the risk, as far as possible, of students being exposed to potentially illegal or inappropriate sites.

5.1.2. Access should be monitored to ensure that no inappropriate or illegal activity has taken place and to help maintain system integrity.

5.2. ICT Support have the right, on the School network, to change any user's password or access rights if they deem it necessary and to report to the Deputy Headmaster, as Online Safety Officer, any inappropriate access they may discover.

5.3. The School's ICT Support should routinely report on the level of monitoring and of incidents arising.

5.4. School data should generally not leave site and if it must leave site it should be encrypted. Any loss of data should be reported immediately.

5.5. The use of the School's network and access to data and information remotely is subject to this Policy and the same rules as if onsite.

5.6. The School's ICT Support will authorise access to the network and devices only through a properly enforced password protection policy, in which passwords are regularly changed. The School's password protocols must be followed. All users will have clearly defined access rights.

5.7. The right to privacy is reduced in any circumstance where safeguarding or welfare of students may be compromised whether this is through the School's own network or on personally owned equipment.

6. Staff

6.1. All staff and volunteers should adhere to the Email and Internet Use Policy and the Password Policy, act in accordance with the School's Code of Conduct and be good role models in their use of ICT, the internet and mobile devices.

6.2. Online safety issues will be embedded in all aspects of the curriculum and other school activities. Staff must monitor ICT activity in lessons, extra-curricular and extended school activities including in boarding time. Staff should ensure that in using ICT in teaching, prep or other school activities students:

6.2.1. Understand and follow the School's online safety rules, including those in the School's Behaviour Policy, and the Acceptable Use Agreement.

6.2.2. Have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

6.3. Any online safety incident is to be brought to the immediate attention of the Deputy Headmaster as Online Safety Officer, or in his absence the Headmaster, who will deal with the matter.

7. Acceptable Use Agreement

7.1. Students and staff are required to sign the School's Acceptable Use Agreement.

7.2. Visitors will be informed of the School's Acceptable Use agreement on arrival.

7.3. All users of the School's computer equipment and internet connections will be reminded of the Acceptable Use requirement, and required to acknowledge that that have been so reminded, by accepting a simplified code of conduct each and every time they log on to the School's systems.

7.4. Use of the School's internet and devices is intended for school business or professional development. Any personal use is subject to the same terms and conditions and is only in accordance with the student/staff use policies or with the agreement of the Headmaster.

8. Application of this Policy

8.1. Governors acknowledge that technology continues to advance rapidly however their responsibility to safeguard and promote the welfare of students remains constant as do the underlying principles of online safety. The School will develop the principles of this Policy to a sufficient degree to provide a working document that will set out and explain how the School applies these principles in practice.

8.2. Governors acknowledge the application document will change from time to time, not least because this is a fast evolving area with new technologies emerging at a pace but also, because it is an operational document. The Headmaster will maintain the application document, reporting any significant changes as they are made and reporting lesser and all routine changes during the annual policy review.

8.3. A copy of the application document current at the date of the policy review is attached.

Application of Online Safety and Computer Usage Policy

1. Introduction

This document seeks to apply the approved Policy and support the aims of the School in educating students to explore their horizons by using online devices and technologies and by doing so with safety, caution and responsibility for themselves and with respect for others[4].

2. References:

This document references the following school policies and other guidance and should be used in conjunction with them:

Policies:

- Behaviour Policy including the School Rules, Code of Conduct for Students, School Dress Code, Regulations for Registration, Absence and Leaving School Grounds, Rewards & Sanctions, Anti-Bullying, Drugs/Substance Use and Misuse, and Student Use of Electrical and Electronic Equipment & Internet Guidance
- Boarding Policy
- Code of Conduct for Staff & Volunteers
- Data Protection Policy
- Email and Internet Usage Policy
- Information Security Policy
- Online Safety and Computer Usage Policy
- Password Policy
- Publication Scheme on Information Available under the Freedom of Information Act
- Safeguarding Policy

Guidance:

- DSCB Safeguarding Children Procedures - http://safeguarding.dudley.gov.uk
- Working Together to Safeguard Children (March 2015)
- Keeping Children Safe in Education (September 2016)
- Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (March 2015)
- What to do if you're worried a child is being abused: Advice for practitioners (March 2015)
- Guidance for Safer Working Practice for those Working with Children and Young People in Educational Settings (October 2015)
- Sexting in schools & colleges: responding to incidents and safeguarding young people (August 2016)
- DCSB Use of Images Guidance
- Revised Prevent Duty Guidance: for England and Wales (July 2015)
- The Prevent Duty: Departmental advice for schools and childcare providers (June 2015)

[4] For the purposes of this document any reference to the internet and or electronic devices (or these technologies in general) will include all access to technology based information or methods of communication including the use of the School's network and any of its devices (either linked or standalone), the use of own or third party devices for any form of internet access, means of communication or other associated use including but not limited to the use of 'Cloud ' based provision and any form of social media.

3. Rationale

3.1. ICT is 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 equip children and young people with the skills to access life-long learning and employment.

3.2. 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
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

3.3. Whilst exciting and beneficial both in and out of the context of education, users need to be aware of the range of risks associated with the use of these internet technologies.

3.4. The School understands its responsibility to educate students in online safety; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legally compliant when using the internet and related technologies, in and beyond the context of the classroom.

3.5. Schools hold personal data on students, 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 the School to use technology to benefit learners. All staff have 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.

3.6. Both this document and the Acceptable Use Agreements for all students, staff and visitors (Annex A, B and C attached) are inclusive of, but not limited to, fixed and mobile internet; technologies provided by the School (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students, staff[5], and visitors[6], but brought onto school premises (such as laptops, mobile/smart phones, tablets, MP3 players, etc.).

[5] References to staff will include supply and temporary staff and volunteers.

[6] References to visitors will include contractors and parents.

4. Roles and Responsibilities

4.1. Online safety is an important aspect of strategic leadership within the School and the Headmaster and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

4.2. The School's Online Safety Officer is Dale Wilkins, the Deputy Headmaster. All members of the school community have been made aware of who holds this post.

4.3. It is the role of the Online Safety Officer to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection), Childnet and others.

4.4. Whilst Governors have overall responsibility for safeguarding and promoting student welfare and well-being at the School protecting students and securing their welfare is also the responsibility of all staff.

5. Monitoring

5.1. Authorised ICT staff may inspect any school ICT equipment[7] at any time without prior notice. To verify the authority for any such request contact the School's ICT Manager.

5.2. To the extent permitted in law, authorised ICT 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 students, staff or visitors, without consent. This may be to confirm or obtain School business related information; to confirm or investigate compliance with the School's 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.

5.3. Authorised ICT staff may, with the permission of the Headmaster or the Deputy Headmaster, 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.

5.4. 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.

5.5. Personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

6. Breach of Policy[8]

6.1. Response to a Breach of Policy

6.1.1. A breach or suspected breach of policy by a student, member of staff or visitor may result in the temporary or permanent withdrawal of school ICT hardware, software or services from that individual/those individuals.

6.1.2. Any policy breach is grounds for disciplinary action in accordance with the School's Behaviour Policy or Disciplinary Procedure as appropriate.

6.1.3. Policy breaches may also lead to criminal or civil proceedings.

[7] However owned, leased, rented or made available to the School.

[8] For the purpose of defining a breach of the School's Policy for Online Safety and Computer Use this document, which sets out the application of that Policy, shall have the same standing as the Policy to which it refers. Therefore any breach of matters referred to in this document shall be taken to be a breach of the School's Policy.

6.2. Incident Reporting

6.2.1. 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 ICT Manager in the first instance. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Deputy Headmaster as the Online Safety Officer (or, in his absence, the duty member of Senior Leadership Team (SLT) on call).

6.2.2. All online safety incidents involving either students or staff should be recorded on the online safety incident log by the Headmaster's PA.

6.2.3. Should a concern be about internet safety for students there is a link on the VLE (Frog) to the CEOP[9] website where information and guidance can be sought. Concerns can also be raised directly with the Deputy Headmaster (as Online Safety Officer and DSL) or optionally this may be done using the anonymous online reporting system in Frog.

6.3. Complaints and/or Issues

6.3.1. Complaints and/or issues relating to online safety should be made to the Deputy Headmaster as Online Safety Officer.

6.3.2. Complaints will be dealt with in accordance with the School's Complaints Policy or staff Grievance Procedure as appropriate.

6.3.3. All incidents should be logged and the School's procedure for investigating incidents and recording complaints should be followed.

6.4. Inappropriate Material

6.4.1. Accidental access to inappropriate materials must be immediately reported to the Deputy Headmaster, as Online Safety Officer and DSL or a member of the SLT if he is unavailable.

6.4.2. Deliberate access to inappropriate materials will lead to the incident being logged by the Deputy Headmaster depending on the seriousness of the offence; investigation by the Deputy Headmaster or Headmaster, immediate suspension, possibly leading to exclusion/dismissal and, where appropriate, referral to external agencies including the National College of Teachers and the police for very serious offences.

7. Inclusion

7.1. Students may join the School with varied and different understandings of online safety. The School endeavours to create a consistent message with students and parents[10] which in turn should help establish, cement and further develop the Schools' online safety rules.

7.2. Staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

7.3. Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children and young people.

[9] The National Crime Agency's CEOP Command (formerly the Child Exploitation and Online Protection Centre) works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account and protect children from harm online and offline.

[10] Any reference to parent includes carer.

8. Computer Viruses

8.1. It important that students and staff never interfere with any anti-virus software installed on school ICT equipment. Any interference will be treated as a serious breach of policy.

8.2. Provision for regular virus updates must also be made.

9. Data Security

Please see our Data Protection and Password policies.

10. Student and Staff Education and Training

10.1. Online Safety in the Curriculum

10.1.1. ICT and online resources are increasingly used across the curriculum so it is essential for online safety guidance to be given to the students on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety. The School has a framework for teaching internet skills in ICT/PD lessons and tutorial sessions. Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.

10.1.2. Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them. Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.

10.1.3. Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

10.1.4. Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

10.1.5. Whole school assemblies are also used to keep current the understanding and importance of online safety.

10.2. Online Safety Skills Development for Staff

10.2.1. New staff receive information on the School's acceptable use policy as part of their induction.

10.2.2. All staff must be aware of individual responsibilities relating to the safeguarding of students within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

10.2.3. All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas.

10.2.4. Information and training updates on online safety issues are provided.

10.2.5. Staff complete Prevent awareness training in order to become more familiar with the signs and symptoms of extremism and appropriate responses to it.

10.3. Online Safety Forum for Students

10.3.1. The School Council provides an additional opportunity for students to comment on what is currently happening such as new sites arising, security settings that need pointing out, what is used for bullying e.g. ASK FM, SNAPCHAT etc.

10.3.2. The School Council also provides a forum to meet to discuss our ICT expectation, policies, website filtering, identify hate emails and teach the effect of this, provide technology ideas, all providing a greater understanding at both the staff and student level.

11. Systems and Access

11.1. Guiding Principles and Regulations

11.1.1. All staff are responsible for any activity on school systems carried out under access/account rights assigned to them, whether accessed via school ICT equipment or their own PC.

11.1.2. No member of staff should allow any unauthorised person to use school ICT facilities and services that have been provided to them.

11.1.3. Staff should use only their personal logons, account IDs and passwords and not allow them to be used by anyone else.

11.1.4. Screen displays should be kept out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

11.1.5. Staff should ensure they log off before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

11.1.6. Staff should not introduce or propagate viruses knowingly.

11.1.7. It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the School or may bring the School into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the School's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

11.1.8. Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act.

11.1.9. Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

11.2. E-mail

11.2.1. Please see the separate Email and Internet Use Policy for staff.

11.2.2. The use of e-mail within most schools is also an important means of communication for students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of

appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

11.2.3. Students are introduced to e-mail as part of the ICT Scheme of Work. However school e-mail is accesses, (whether directly, through webmail when away from the office or on non-school hardware) all the School's e-mail policies apply.

11.3. Internet Usage

11.3.1. 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.

11.3.2. All use of the internet at the School is logged and the logs are randomly but regularly monitored. This also applies to school based email activity.

11.3.3. The School does not allow students access to internet logs.

11.3.4. The School uses management control tools for controlling and monitoring workstations.

11.3.5. Whenever any inappropriate use of equipment or internet activity is detected it will be followed up.

11.3.6. Raw image searches are discouraged when working with students.

11.3.7. All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

11.3.8. All users must observe copyright of materials from electronic resources.

11.3.9. Personal, sensitive, confidential or classified information must not be posted or disseminated in any way that may compromise its intended restricted audience.

11.3.10. Names of colleagues, students or parents, or any other confidential information should not be revealed on any social networking site or blog.

11.3.11. On-line gambling is not allowed.

11.3.12. The School's ICT Manager will maintain and update anti-virus protection on all school machines.

11.3.13. Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the School's or the ICT Manager's responsibility to install or maintain virus protection on personal systems.

11.3.14. Students and staff are not permitted to download or upload programs on school based technologies without prior permission from the ICT Manager.

11.3.15. If there are any issues related to viruses or anti-virus software the ICT Manager should be informed immediately.

11.4. Managing Web 2.0 Technologies

11.4.1. Web 2.0, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. They have a particular value to boarding schools where parents can live some distance from site and who boarders only see at holiday times.

11.4.2. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. Students are encouraged to think

carefully about the way that information can be added and removed by all users, including themselves, from these sites.

11.4.3. The School allows limited access to these sites on the school network during boarding time.

11.4.4. The School filters access to the internet to reduce the risk, as far as possible, of students being exposed to potentially illegal or inappropriate sites. The School's filtering software blocks access to certain chat rooms, newsgroups and websites and filters for the use of unsuitable or inappropriate words/phrases including in emails. The filtering of emails also includes those potentially carrying a virus or appearing to be spam email such as a phishing message.

11.4.5. The School monitors access to ensure that no inappropriate or illegal activity has taken place and to help maintain system integrity. The School's ICT Support will carry out the routine monitoring of use and reporting of incidents. User areas on the School's network will be closely monitored. The School's ICT Support have the right, on the School's network, to change any user's password or access rights if they deem it necessary and to report to the Deputy Headmaster, as Online Safety Officer, any inappropriate access they may discover.

11.4.6. All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

11.4.7. Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

11.4.8. Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

11.4.9. Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals and encouraged to be wary about publishing specific and detailed private thoughts online.

12. Protecting Personal, Sensitive, Confidential and Classified Information

All users should:

12.1. Ensure that any school information accessed from personal equipment or removable media equipment is kept secure.

12.2. Log off before moving away from a computer during the normal working day to prevent unauthorised access.

12.3. Ensure the accuracy of any personal, sensitive, confidential and classified information disclosed or shared with others and that it is not disclosed to any unauthorised person.

12.4. Ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

12.5. Not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

12.6. Keep screen displays out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

12.7. Ensure hard copies of data are securely stored and disposed of after use.

13. Safe Use of Images[11]

13.1. Digital images are easy to capture, reproduce and publish and, therefore, misuse. 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.

13.2. As a default, students must not take pictures of other students.

13.3. With the written consent of parents (on behalf of students) and staff, the School permits the appropriate taking of images by students and staff with school equipment.

14. ICT Equipment Within School

14.1. PCs, Laptops, Tablets and Other School Equipment

14.1.1. Students are responsible for their activity on the School's ICT equipment.

14.1.2. Unauthorised access to, or modifications of, computer equipment, programs, files or data is not permitted. This is an offence under the Computer Misuse Act 1990.

14.1.3. It is imperative that data is saved to the School's network on a frequent basis. Users are responsible for the backup and restoration of any of their data that is not held on the School's network drives.

14.1.4. Users are responsible for ensuring that any information accessed from your own PC, Laptop or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

14.1.5. All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

14.1.6. Staff must ensure that all school data is stored on the School's network, and not kept solely on a laptop.

14.1.7. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes including when travelling.

14.1.8. Portable and mobile ICT equipment must be made available as necessary for anti-virus updates and software installations, patches or upgrades.

14.1.9. The installation of any applications or software packages must be authorised by the ICT team, fully licensed and only carried out by ICT Support.

14.1.10. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

14.1.11. Portable equipment must be transported in its protective case if supplied.

14.2. Mobile Technologies

14.2.1. 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, tablets, gaming devices, mobile/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.

[11] For full information see DSCB guidance: Use of Images Guidance

14.2.2. The School manages the use of these devices in the following ways so that users exploit them appropriately:

14.2.2.1. Staff are permitted to bring in personal mobile phones and devices for their own use. Under no circumstances does is a member of staff permitted to contact a student or parent using their personal device unless it is for the purpose of enhancing their duties (e.g. contacting a student with information during a school trip).

14.2.2.2. Students are allowed to bring personal mobile devices/phones to school but must turn them off during lesson time. This technology may be used, however for educational purposes, as mutually agreed with the Second Deputy and Subject Leader and so long as the School's wireless network is being used.

14.2.2.3. The School is not responsible for the loss, damage or theft of any personal mobile device.

14.2.2.4. The sending of inappropriate text messages between any members of the school community is not allowed.

14.2.2.5. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

14.2.2.6. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

15. Sanctions for Students

Sanctions referenced in the Behaviour Policy may be used in order to deal with misuse of information technologies or inappropriate, offensive or dangerous online behaviours.

Appendix A

Students' Acceptable Use Agreement

How I use technology at Old Swinford Hospital

I DO:

- Use the computers to help me research topics for my work
- Use the computers to make pieces of work look well presented
- Use the computers to communicate with members of staff if I need to be excused from lessons
- Use the computers to communicate with members of my family if I don't see them very often i.e. if I am boarding or if my parents go away during term time
- Ask a member of staff if I am unsure whether I should be doing something or not or if I need help
- Tell a member of staff immediately if I feel uncomfortable or threatened by anything that I see on the internet or receive in an e-mail
- Send e-mails or messages that are polite and are not offensive or discriminatory
- Keep my personal information and passwords safe and I will not give them out to anyone
- Know how to look after myself and my friends by using the internet in a safe and responsible way

I DO NOT:

- Use language on the internet or in emails that I would not use in front of a teacher
- Use other people's passwords; this includes attempting to log in through another person's account or accessing another person's files

I UNDERSTAND THAT:

- Using other people's work and claiming that it is my own is a crime
- Any persistent abuse of the School's computer systems will result in my access being suspended or permanently removed
- Cyber-bullying is when a person or a group of people threaten, tease, embarrass or abuse someone else by using ICT, particularly mobile phones, the internet and related technologies such as social networks
- Cyber-bullying will be dealt with as seriously as any real world bullying incident

Continued overleaf

Guidance for Students

Staying safe

If at any time you feel unsafe using a computer then find a responsible adult straight away and make sure that the Deputy Headmaster, your Housemaster or your Tutor are made aware of what is happening.

School Directory

Every student in the School is given an area on the Old Swinford Hospital's server system to store their work and other important files. This area is not to be used for storing movies, photos, videos, personal music files or computer games.

What you can expect to happen if you do not follow these rules

If any member of staff feels that there has been a breach of these rules then the ICT department will investigate the matter fully and accounts will be suspended or deleted if necessary. Appropriate action will also be taken in line with the School's Behaviour Policy. Any form of cyber-bullying is regarded as an exceptionally serious offence.

I agree to the Terms and Conditions of the Students' Acceptable Use Agreement

Signed: …… Print Name: …… Date: ……

Appendix B

Staff Code of Conduct for the Use of ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the School's document Application of Online Safety and Computer Use Policy for further information and clarification.

1. **I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.**
    - I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business
    - I understand that school information systems may not be used for private purposes without specific permission from the Headmaster
    - I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager
    - I will not install any software or hardware without permission
    - I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely
    - I will respect copyright and intellectual property rights.
2. **I understand that it is my duty to promote online safety with students in my care, to report any matters of concern, and to use electronic communications of any kind in a professional and responsible manner.**
    - I will promote online-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing
    - I will report any incidents of concern regarding student safety to the Deputy Headmaster or a member of the SLT.
    - I will ensure that electronic communications with students including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
3. **I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.**

The School may exercise its right to monitor the use of the School's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read and understand the School's Online Safety and Computer Use Policy and the School's document Application of Online Safety and Computer Use Policy and I agree to abide by both and to the Terms and Conditions of the Staff Code of Conduct for the use of ICT

Signed: …… Print Name: …… Date: ……

Appendix C

Visitor Code of Conduct for the Use of ICT

To ensure that all visitors are fully aware of their responsibilities when using information systems, they are asked to sign this code of conduct. Visitors may consult the School's document Application of Online Safety and Computer Use Policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner
- I appreciate that ICT includes a wide range of systems, including mobile phones, Tablets, digital cameras, e-mail and social networking, and that ICT use may also include personal ICT devices when used for school business
- I understand that school information systems may not be used for private purposes without specific permission from the headmaster
- I understand that my use of school information systems, Internet and e-mail may be monitored and recorded to ensure policy compliance
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager
- I will not install any software or hardware without permission
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely
- I will respect copyright and intellectual property rights
- I will report any incidents of concern regarding student safety to the Deputy Headmaster (Online Safety Officer and Designated Safeguarding Lead)
- I will ensure that electronic communications with students including email, IM and social networking are compatible with my role for the School and that messages cannot be misunderstood or misinterpreted
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing

The School may exercise its right to monitor the use of the School's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix D

Current Legislation

1. 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. **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 Human Rights Act 1998**

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.

2. Other Acts Relating to online safety

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.

All staff should be aware of the Keeping Children Safe in Education[12].

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:

i. Access to computer files or software without permission (for example using another person's password to access files)

[12] The current version is dated September 2016. Staff will be expected to routinely keep up to date with any subsequent editions.

ii. Unauthorised access, as above, in order to commit a further criminal act (such as fraud)
iii. 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 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.

3. Acts Relating to the Protection of Personal Data

Data Protection Act 1998

The Freedom of Information Act 2000