DIGITAL TECHNOLOGIES and ONLINE SAFETY POLICY

LSA Technology and Performing Arts College is committed to safeguarding and promoting the welfare of young people and expects all staff and volunteers to share this commitment.

Contents

1 Introduction

1.1 Digital Technologies are a great resource to support learning and teaching, playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build on the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. This policy is to ensure we protect and educate students and staff in their use of technology. Also to ensure we have the appropriate mechanisms to intervene and support incidents where appropriate.

1.2 Digital Technologies are constantly evolving and young people are using the following both inside and outside of the classroom

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile phones
- Mobile devices eg tablets

1.3 All users need to be aware of the range of risks associated with the use of these digital technologies.

1.4 At LSA we understand the responsibility to educate our students about online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.5 Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of the internet (including the Guest and Tablets network); technologies provided by the school (such as PCs, laptops, 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 and mobile devices etc).

2 Roles and Responsibilities

2.1 As Digital Technology and Online Safety are 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 Online Safety Co-ordinator in our school is the Head of Computing, directly responsible to the Assistant Head. The Assistant Head also chairs the ICT Strategy Group which has responsibility for online safety. All members of the school community have been made aware of who holds these posts. It is the role of the Online Safety Co-ordinator to keep abreast of current issues and guidance.

2.2 Senior Management and Governors are updated by the Online 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.

2.3 This policy, supported by the school's acceptable use, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding & Child Protection, Health and Safety, home–school agreements, and Behaviour/student discipline (including the Respect & Anti-Bullying) policy.

2.4 Online Safety Skills Development for Staff

- Our staff receive regular information and training on online safety issues in the form of briefings and training sessions.
- Details of the ongoing staff training programme can be found in the Training Tuesday programme on the X drive
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children 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.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas as it is everyone's responsibility.

2.5 Managing the School Online Safety Messages

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Online Safety Policy will be introduced to the students at the start of each school year.
- Online safety posters will be prominently displayed.

3 Digital Technology and Online Safety in the Curriculum

3.1 Digital Technologies are increasingly used across the curriculum. We believe 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, including activities in Life lessons.

3.2 The school has a framework for teaching internet and online safety skills in KS3 Computing lessons.

3.3 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. As technologies and their issues evolve we change to support this eg teaching about Sexting/SGII in Yr9.

3.4 Students are made aware of the relevant legislation in KS3 Computing lessons e.g. data protection and the use of intellectual property. This may limit what they want to do e.g. copy images from the internet, but also serves to protect them. They are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

3.5 Students are made aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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/ carer, teacher/ trusted staff member, or an organisation such as Childline.

3.6 Students are taught to critically evaluate materials and learn good searching skills in all subjects.

4 Password Security

4.1 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. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security. If you think your password may have been compromised or someone else has become aware of your password report this to the ICT technical team immediately.

4.2 Users are provided with an individual network, email and Learning Platform log-in username. They are expected to use a password and keep it private. Logging on as someone else is not permitted.

4.3 Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked as appropriate. For best practice, prompts to 'remember password' should not be ticked, especially on shared devices.

5 Data Security

5.1 The accessing and appropriate use of school data is something that the school takes very seriously.

5.2 Staff are aware of their responsibility when accessing school data, with the level of access determined by the Head Teacher.

5.3 Any data taken off the school premises **must** be secure. The ICT technical team will provide support in this area

5.4 Data can only be stored and used on school computers or laptops. Any school data accessed via email on personal devices should ensure sufficient security and privacy if used outside the school.

6 Managing the Internet

6.1 The internet is both an invaluable resource for education and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

6.2 The school maintains students will have supervised access to Internet resources through the school's Wifi, including the Guest network for devices.

6.3 Staff will preview any recommended sites before use, raw image searches are discouraged when working with students, due to the possibility of students viewing unsuitable images.

6.4 If Internet research is set for homework, specific sites should be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.

6.6 All users must observe software copyright at all times. Software free for personal use might not be free for school use.

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

6.8 Infrastructure

- School internet access is controlled and filtered through the local authority's web filtering service.
- LSA is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and students are aware that school based email and internet activity can and will be monitored and explored further if required.
- The school does not allow students access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the most relevant person, e.g. Online Safety Co-ordinator, Head of Department, Technicians, Child Protection Officer. This allows the situation to be dealt with and if appropriate, the site blocked.
- It is the responsibility of the school, by delegation to the Service Provider (Dataspire), to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- 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 responsibility to install or maintain virus protection on personal systems
- Students and staff are not permitted to download programs on school based technologies without seeking prior permission from the ICT technical department.
- If there are any issues related to viruses or anti-virus software, in the first instance the Head Technician should be informed

7 Social Networking

7.1 Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. This is supported in Computing lessons, as well as other curriculum activities.

7.2 The school endeavours to deny access to any social networking sites to students within school, with the exception of those specifically classified as educational.

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

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

7.5 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).

7.6 Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

7.7 Students are encouraged to be wary about publishing specific and detailed private thoughts online.

7.8 Our students are asked to report any incidents of online bullying to the school. These will be investigated and dealt with as appropriate.

7.9 Staff may only create social network profiles, blogs, wikis or other Internet communication tools in order to communicate with students with prior consent from the Assistant Head responsible.

7.10 The open nature of social networking means that staff should take active steps to protect themselves. Anything posted online is potentially public and permanent even when privacy settings are used. Our staff are advised to set and maintain profiles on any social networking etc sites they use outside school to maximum privacy and deny access to unknown individuals. Access to current students and parents must be denied. Friend requests from previous students should also be refused. By accepting such requests, you could be making yourself vulnerable and could leave yourself open to allegations of inappropriate contact or conduct.

7.11 Staff should think carefully before posting online information about school, staff, students or parents, as comments could be taken out of context and may be very damaging. Staff should also think carefully about how they present themselves when posting images, joining groups or 'liking' things, as these choices will say something about you. Inappropriate posts could be seen as lowering the reputation of LSA and could be a basis for disciplinary action.

For further guidance please see ASCL Guidance Paper 117 "Social Networking and Social Media – Guidance for members"

8 Mobile technologies

8.1 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. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school approaches this positively and chooses to manage the use of these devices in the following ways, so that users exploit them appropriately.

8.2 Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. Generally the device must be switched onto silent.
- Student devices may be used however for educational purposes, as laid out it the Student Mobile Phone/Device policy. Monitored internet access is allowed via guest login.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages and images (this includes sexting, see appendix A) between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community (also see Section 10)
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. This can be hard to monitor and staff need to be aware of this. Students also need to be aware of their responsibility.

8.3 School Provided Mobile Devices (including phones)

- The sending of inappropriate messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips only these devices should be used.

9 Managing email

9.1 The use of email is an essential means of communication for both staff and students, but should **not be considered private**. We recognise that students need to understand how to style an email in relation to their age and good netiquette. A part of the Computing Curriculum, students will experience sending and receiving emails in an appropriate manner.

9.2 The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

9.3 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business. Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.

9.4 A standard disclaimer is attached to all external email correspondence, stating that, ‘the views expressed are not necessarily those of the school or the LA’.

9.5 E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

9.6 Students use school approved accounts on the school system, under direct teacher supervision for educational purposes. It may be appropriate for them to use personal email at times and again this should be supervised.

9.7 All 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 and being wary of attachments.

9.8 Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail. Staff must inform the Online Safety Co-ordinator and line manager if they receive such emails.

10 Safe Use of Images

10.1 Taking of Images and Film

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

- The school permits the appropriate taking of images by staff and students with school equipment unless parents have 'opted out' of this permission.
- Staff are not permitted to use personal equipment, to record images of students, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Staff are reminded that not all students or staff will be comfortable having their photo taken and their permission should also be gained, especially if the photo is intended for a wider audience.

10.2 Consent of adults who work at the school

Before including any members of staff, visitors or parents in photos, their permission must be sought. We should not assume that adults are happy for their photo to be circulated to a wide audience.

10.3 Publishing student's images and work

On a child's entry to the school, all parents/guardians will be asked to inform the school if they do not give permission for their child's work/photos to be displayed. This consent is considered valid for the entire period that the child attends this school. Parents/ carers may withdraw permission, in writing, at any time.

Before posting student work on the school website or Moodle, a check needs to be made to ensure that permission has been given for work to be displayed.

10.4 Storage of Images

Images/ films of children are stored on the school's network. Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher. Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform. Cameras can be used effectively in lessons, with images safely transferred to the network as soon as possible.

10.5 Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are members of staff nominated by the Headteacher**.**
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

10.6 Video Conferencing

- Video conferencing facilities such as Skype are used as an effective educational tool**.** All exchanges are planned and all students are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

11 Misuse and Infringements

11.1 Complaints

Complaints relating to Digital Technologies should be made to the Online Safety Co-ordinator, the Head Teacher or the Assistant Head responsible. Incidents should be logged and dealt with according to the most appropriate school policy and logged using the Incident Log at section 17.

11.2 Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Co-ordinator and possibly the Safeguarding Team.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator and depending on the seriousness of the offence, investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to misuse

12 Equal Opportunities

12.1 Students and staff with additional needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the school's online safety rules.

However, 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.

Where a student has been identified as having 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.

13 Parental Involvement

13.1 We believe that it is essential for parents/ carers to be fully involved with promoting online safety both in and outside of school. We regularly seek to advise parents/carers of the benefits related to ICT use and the associated risks.

13.2 Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

13.3 Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

13.5 The school disseminates information to parents relating to online safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website/ Learning Platform postings
- Newsletter items
- Participation in some homework activities
- Twitter feeds

14 Writing and Reviewing this Policy

14.1 Staff and student involvement in policy creation

Staff, students and Governors have been involved in making/ reviewing the Online Safety Policy through consultation.

14.2 Review Procedure

There will be an on-going opportunity for staff to discuss with the Online Safety Coordinator any issue of online safety that concerns them.

This policy will be reviewed as part of the cycle of policy review and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

15 **Acceptable Use Policy of Digital Technologies Agreement: Staff, Governors and Visitors**

Digital Technologies such as email, the internet and mobile devices, are an expected part of our daily working life in school. This document is designed to ensure that all staff are aware of their professional responsibilities when using any form of Digital Technology. All staff are expected to sign this policy and adhere, at all times, to its contents. Any concerns or clarification should be discussed with the Assistant Head responsible or the School Online Safety Coordinator.

- I will only use the school's email / Internet / 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, parents, staff and other stakeholders are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only communicate with students via school approved channels
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission from ICT support
- 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. Images on devices need transferring to the network as soon as is possible.
- I understand that all my use of the Internet and other related technologies during school time or on school equipment can and will be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- 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.
- Any YouTube clips or other online video source will be checked prior to lessons.
- I will support and promote the school's online safety policy 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 use of Digital Technologies throughout the school. When I sign the safeguarding proforma, I am stating that I understand and accept this policy and this impact it has on my practice.

Signature …….…… Date ……

Full Name …….....(printed)

16 LSA Student Code of Conduct for use of Digital Technologies in school

- I will only use Digital Technologies in school, such as the Internet, email, video and mobile technologies for school purposes.
- I will not download or install software onto the school network/computers.
- I will only log on to the school network and Learning Platform with my own user name and password.
- I will not reveal my passwords to anyone and change them when needed.
- I will only log into my own accounts. I will not access or interfere with other students' accounts and/or work.
- I will make sure that all electronic communications with students, teachers or others is responsible and sensible.
- I understand that I cannot contact any member of the school staff using their **personal** accounts such as: Facebook, twitter, internet gaming sites or any other social networking site
- I understand I can only contact members of staff electronically on their school email and school approved education channels.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not use the Internet to play games in lessons.
- When online I will not give out any personal information such as my name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will only take photos of staff or students with their permission and when needed for my work. I will store and use them sensibly.
- I will not copy work that I have found online and say it is mine.
- I will not attempt to get round the internet filtering system.
- I understand that all my use of the Internet and the school computers can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school consequences will be applied and my parent/ carer may be contacted.

If you think your password is known by somebody else, please change it immediately by contacting the school technicians

I understand the code of conduct and I agree to follow it

Signature …….…… Date ……

Full Name …… (printed) Form …….

17 Using Education Websites that offer a Social Aspect

Many amazing websites exist that allow us to communicate effectively with our students, such as Edmodo or Showbie. They are greeted positively by the students as they offer an environment that seems to replicate that of a social network but within a more controlled setting.

However, as these websites are outside the school's control they don't offer as much protection to students or staff. For instance, currently Moodle is the school's VLE; all communications that occur are recorded and could be monitored if required.

With this in mind, if groups are set up with students on educational websites there **must** be 2 staff members. This will help both support and protect staff eg reinforcing the language expectations and, spotting if any students need further support. It can be hard to judge the tone of electronic communication and having at least 2 members of staff in groups would help pick up on conversations that were less appropriate, enabling them to be dealt with promptly.

Staff should not use such websites to connect with and message students as individuals. Messaging a student individually through the group is fine as a record of this communication can easily be seen. However, if you connect with a student individually this communication will only be seen by you and breaches our Social Networking policy. Such communications could be a safeguarding issue, both for you and the students.

18 Using Twitter to Communicate with Parents and Students

Twitter is a great communication tool and its use in school is generally greeted really positively by staff, students and parents alike. It allows a much wider community access to what we do and this can provide access to great opportunities. Parents/carers can experience in real time what their child is doing on a trip, how their science experiment is going, helping to engender an increased sense of community. However, we must remember that Twitter is a social networking tool and with this in mind there are procedures that must be in place to prevent safeguarding issues both for staff and the students.

1. So there is no room to blur the lines between personal and LSA use of Twitter, any account that is being used to communicate school news must be a recognised school account rather than a personal one. So accounts should follow the naming convention of @LSAGeography, @LSABusiness, @LSADigital etc.

   This is especially important if any images of the students are used – school has permission to use these on such media whereas individual members of staff do not. Staff must also check that use of an individual's photograph is allowed and should refer to sections 10.1-10.4 of the Digital Technology policy for further information.
   Again there **must** be at least 2 staff who can access the departmental Twitter. This could be through joint ownership of the account or by following the

account so you can see the tweets. Any views or comments expressed must reflect that of the school and it's worth looking at section 7.11 of the Digital Technology policy for further clarification

2. If you have a personal Twitter account which you are using for work purposes the Digital Technology policy applies in the same way, so you should not have current parents or any students (past or present) following you, nor should you follow them. This would seem to negate the reason for you having it and creates a stronger reason to create a departmental one.

3. The departmental Twitter should follow @lythamhigh and this will help highlight your existence to people interested in school news

4. COPA (Child Online Protection) states that the minimum age for a Social Networking account is 13. Whilst departments cannot be held responsible for the age of their followers, if it's obvious, those under 13 should be deleted.

Next steps for Twitter

- Decide on the name for your departmental Twitter – following the school policy of @LSA
- Does someone already operate a departmental Twitter where you could just amend the name?
- Decide who will run the Departmental Twitter – making sure there are at least two
- Set it up!
- Follow @lythamhigh and all the other departmental Twitters that you like the sound of!

19 Current Legislation

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

20 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. 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 person's 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 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.

Last review: **March 2017**
Next review: **March 2018**

APPENDIX A

Dealing with Incidents of Sexting

1 What is sexting?

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. Young people may get involved in sexting without thinking about the consequences or they could be coerced into it (possibly as Child Sexual Exploitation).

2 Why do young people sext?

There are many reasons why a young person may want to send a naked or semi-naked picture, video or message to someone else:

- joining in because they think that 'everyone is doing it'
- boosting their self-esteem
- flirting with others and testing their sexual identity
- exploring their sexual feelings
- to get attention and connect with new people on social media
- because they find it difficult to say no if somebody asks them for an explicit image, especially if the person asking is persistent

3 The Law

Sexting can be seen as harmless, but creating or sharing explicit images of a child (under 18) is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

However, as of January 2016 in England and Wales, if a young person is found creating or sharing images, the police can choose to record that a crime has been committed but that taking formal action isn't in the public interest. Crimes recorded this way are unlikely to appear on future records or checks, unless the young person has been involved in other similar activities which may indicate that they're at risk.

Source https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting

4 How A Suspected Sexting Incident Will Be Dealt With In School.

The member of staff who is made aware of the suspected sexting should:

- If a device is involved - confiscate it and set it to flight mode or, if not possible, switch it off. You may decide to call patrol to support with this.
- Report to a Child Protection Officer via normal child protection procedures: CPOMS and verbal contact.

The Child Protection Officer will then decide the action to take, judging each situation independently and considering the following:

- Is there a significant age difference between the sender/receiver involved?
- Is there any external coercion involved or encouragement beyond the sender/receiver?
- Do you recognise the child as more vulnerable than usual i.e. at risk?
- Is the image of a severe or extreme nature?
- Is the situation isolated or has the image been more widely distributed?
- Are there other circumstances relating to either sender or recipient that may add cause for concern e.g. home circumstances?

If any of these circumstances are present, then the situation will be escalated through normal child protection procedures. This includes reporting to the police.

If none of these circumstances are present, the situation will be managed accordingly within the school and without escalating to external services. Details of the incident, action and resolution will be recorded.

Source http://swgfl.org.uk/magazine/Managing-Sexting-Incidents/Sexting-Advice.aspx