MANOR
MULTI ACADEMY TRUST

Policy Document for: e-Safety

Approved by Directors: June 2018

Due for Review: June 2023

Introduction

In today's society, the Internet is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. At Manor Multi Academy Trust, we need to build in the use of these technologies in order to provide our young people with the skills to access life-long learning and employment. Children today are growing up in a technology rich world and as a school we want to embrace and nurture this, however making sure that all members of our school are kept safe from any possible dangers/problems that can be associated with the Internet.

E-safety involves pupils, staff, governors and parents making best use of current technology, information, and training with the main purpose of protecting and safeguarding every member of our school. This policy will set out the parameters to create and maintain a safe online and technology rich environment for all at Manor Multi Academy Trust School.

This policy works alongside the Manor Multi Academy Trust Social Media Policy and the Mobile Device Policy.

Objectives and targets

This policy is aimed at making the use of electronic communication at Manor Multi Academy Trust and its schools as safe as possible. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

Action plan

The MAT schools will deal with any e-safety incidents which arise by invoking this policy, other ICT policies and the associated behaviour and anti-bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school and take appropriate action.

The following sections outline:

- The roles and responsibilities for e-safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles.
- How the infrastructure is managed.
- How e-safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.
- Awareness of and dealing with inappropriate use of electronic media.

Roles and responsibilities – Governors

- Governors will ensure that appropriate filters and monitoring systems are in place on the school's ICT resources.
- Governors will ensure that pupils are taught about e-safety, for example through personal, social, health and economic education (PSHE) and through sex and relationship education (SRE).
- Governors are responsible for the approval of the e-safety policy, for reviewing the effectiveness of the policy and for dealing with issues when they arise.
- A nominated link governor for e-safety is appointed as a member of the school's e-safety committee.
- Governors receive e-safety training/awareness sessions as part of their regular cycle of meetings.

Roles and responsibilities – Executive Head, Heads of School and senior leaders

- The Executive Head is responsible for ensuring the e-safety of members of the school community and will manage the education of pupils and training of staff in e-safety and awareness of potential radicalisation in pupils. (All references to the Head in this document refer to both the Executive Head and Heads of School, except where indicated otherwise)
- The Head and another member of the senior leadership team/e-safety co-ordinator will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including the Head.
- The Education and Inspections Act 2006 empowers the Head, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

Roles and responsibilities – e-safety co-ordinators (Each School nominate)

Leads the e-safety committee.

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy and other related policies.
- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.

- Liaises with the local authority (LA) and reports to the Executive Head any suspicions of pupils who may be becoming radicalised.
- Liaises with school ICT technical staff.
- Reports regularly to senior leadership team.

The e-safety co-ordinator (or other nominated person) will receive training at regular update sessions and by reviewing national and local guidance documents.

Roles and responsibilities – ICT Support Team

ICT Support are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack. That appropriate filters and monitoring systems are in place and fully active
- Academy Schools are adequately backed up and secure
- That the school meets the e-safety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/e-safety policy and guidance.
- That the School operates within Data Protection and GDPR law, ensuring encryption and protection
- Users may only access the school's networks through a properly enforced password protection policy.
- The Executive Head is informed of any suspicions of pupils who may be becoming radicalised

Roles and responsibilities – teaching and support staff

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy.
- They have read, understood and signed where appropriate the relevant staff acceptable usage agreement, and have read other related policies eg mobile phone and social media policies.
- They report any suspected misuse or problem to the e-safety co-ordinator/Head/senior leader/head of ICT/ICT co-ordinator/class teacher/head of year as appropriate for investigation/action/sanction.
- Digital communications with pupils (email/Office 365) should be on a professional level and only carried out using official school systems.
- Pupils understand and follow the school e-safety policy and the pupil acceptable computer usage policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the e-safety issues pertaining to email and social media usage.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They are alert to, and report to the Executive Head, any suspicions of pupils who may be becoming radicalised.

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable usage policies.

Roles and responsibilities – designated person for child protection/child protection officer

The designated person for child protection/child protection officer is trained in e-safety issues and will be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Suspicions of radicalisation

Roles and responsibilities – e-safety group

Members of the e-safety group (link governor, SLT member, staff member, student member, parent representative and ICT technician) will assist with the development of e-safety education.

Roles and responsibilities – pupils

Pupils:

- Are responsible for using the school ICT systems in accordance with the pupil acceptable usage policy and agreement, which they will be expected to sign before being given access to school systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials including suspicions of pupils who may be becoming radicalised, and know how to report such abuse.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.
- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school.

While regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. E-safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT/PSHE/other lessons – this will include both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need for the pupil acceptable computer usage agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils will be taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.

  Rules for use of ICT systems/internet will be posted in all relevant rooms and displayed on log-on screens.

Roles and responsibilities – parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

- Parents and carers will be responsible for endorsing (by signature) the pupil acceptable computer usage agreement.

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- Parents' evenings
- Newsletters
- Letters
- Website
- Information about all relevant national/local e-safety campaigns/literature
- Information about useful organisations /support services for reporting e-safety issues (see appendix 2)

E Safety skills development for staff

Our staff receive regular information and training on e-Safety issues through the
E safety coordinator at staff meetings. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community. New staff receive information on the school's Acceptable Use Agreement as part of their induction. All staff are encouraged to incorporate e-Safety awareness within each of their Computing units of learning, and whenever using the internet to enhance learning opportunities.

E Safety information for pupils and parents/carers

Pupils from Years 1 – 6 are required to sign a differentiated Acceptable Internet Use Agreement. This document is introduced and explained to pupils at the start of each school year and is signed within school. A copy of the Acceptable Internet Use Agreement for Key Stage 1 and 2 pupils is made available to all parents. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the Manor Primary School website/Learning Platform or within any other electronic media form. The children/parent's area of the Manor Multi Academy Trust website/Office 365 system will contain useful information on e-Safety. The school will send out relevant e-Safety information through newsletters

and this will also be displayed on the Manor Multi Academy Trust website/Office 365 system. Age appropriate posters will be displayed in each classroom reminding children about online safety.

Teaching and Learning

Manor Multi Academy Trust will provide opportunities within a range of curriculum areas to teach e-Safety. Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Computing
Curriculum. Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils 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 member of staff, or external agencies. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught how to evaluate Internet content. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Management of infrastructure

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the e-safety policy
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT team and will be reviewed by the e-safety committee (or other group).
- All users will be provided with a username and password by the ICT team
- The 'master/administrator' passwords for the school ICT system, used by the ICT team are also available to the Head or other nominated senior leader and kept in a secure place (eg school safe).
- Users are made responsible for the security of their username and password, must not share or allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by City of Wolverhampton Council (Lightspeed Systems)
- Any filtering issues should be reported immediately to the ICT team
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.
- Monitoring systems across Manor Multi Academy Schools does record all school devices to different levels. More detailed reports can be obtained on desktop and laptop devices and records inappropriate activity within the logs. Apple iPAD devices are secured using a different online monitoring system and can be monitored by activity, location and usage.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other managed devices from accidental or malicious attempts which might threaten the security of the school systems and data.

An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.

- An agreement is signed by members of staff in possession of school provided laptops regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Passwords

Passwords are force to be changed regularly although Pin codes on iPADs are required to be changed by the member of staff regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC / Laptop (using Ctrl, Alt & Del) if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'). The Manor Multi Academy Password Policy is in force across all Academy Schools for authentication and encryption.

Curriculum

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to search the internet freely, eg using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT technician temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Using digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained.

Data protection

From May 2018 personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations

Staff will ensure that they comply with the secure data handling guidelines as specified in the Manor Multi Academy Data Protection Policy and more simply by:

- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.

Protocols for handling electronic communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users will be expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.
- Any digital communication between staff and pupils or parents/carers (email, chat, Office 365 etc) must be professional in tone and content.

Unsuitable/inappropriate activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and e-safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation of pupils

Should any serious e-safety incidents take place, the appropriate external authorities will be informed (eg local area designated safeguarding officer, police etc).

Monitoring and reviewing

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (ie ISP, school network or managed service as appropriate).
- Internal monitoring data for network activity.
- Surveys/questionnaires of pupils, parents/carers and staff.

The policy will be reviewed by the governors, or more importantly, in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to e-safety as advised by the e-safety committee or others.

Use of social networking by staff in a personal capacity.

Some staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner. Please refer to separate **Manor Multi Academy Trust Social Media Policy** for further information.

Use of social networking by parents/carers.

Parents and carers will be made aware of their responsibilities regarding their use of social networking at the beginning of every new school year. Please refer to the **Manor Multi Academy Trust Social Media Policy** for further information. Annual workshops will be held for parents to update them on the use of social media both in school and at home by children/parents and staff.

Cyber Bullying.

Cyber bullying of any member of our Academy Trust community will not be tolerated. Any such incidents, whether on-line or via mobile device, will be dealt with as outlined in the schools Anti-bullying, Behaviour and Safeguarding Children policies. All incidents will be logged by the head teacher the e-Safety subject leader and appropriate support give to anyone in our school community affected by cyber bullying.

All incidents will be recorded on the E-Safety log sheet that is kept by each phase leader. Incidents which may lead to child protection issues need to be passed on to one of the Child Protection Leaders immediately – it is their responsibility to decide on appropriate action.

Incidents which are not child protection issues but may require Leadership Team intervention (e.g. cyberbullying) should be reported to Leadership Team in the same day.

Insurance (Devices)

You will ensure that you will take good care of the iPAD and laptop and take all reasonable precautions to ensure that it is not damaged, lost or stolen. Your laptop has been added to the school's inventory/insurance details. You must ensure that you comply with the following:

- ✓ Laptop & iPAD within School – Your laptop or iPAD must not be left unattended outside the classroom, while it is within school, unless it is securely locked away or the room left in is secure.
- ✓ Laptop & iPAD within your Home – Your laptop or iPAD must never be left on public view within your home. Ensure your home is a safe and secure environment for the work devices. Ideally hide or lock away when not in use. Please add the laptop and / or iPAD to your home insurance policy.

- ✓ Laptop & iPAD – The laptop or iPAD is only insured during transit between School and your Home or between your Home and School.
- ✓ The laptop or iPAD must never be left unattended within a car, even if it is in your boot.

If your laptop or iPAD is lost or stolen, you must inform Head of School and ICT Support immediately. If the laptop is lost or stolen outside of school it is your responsibility to report this matter to the Police as well as the Head of School and ICT Support. Any Police paperwork should be shown to ICT Support for the Inventory/Insurance purposes.

ICT Health and Safety

There are a number of physical health and safety matters to consider when using technology devices within schools including use of wireless networks, ergonomics, using interactive whiteboards and projectors and the risk of photosensitive epilepsy.

Safe location and supervision of computers in schools

Internet access for pupils in schools should be available on computers that are in highly-used areas of the school such as classrooms, libraries and other learning environments.

Computer screens / laptops should be visible to other people circulating in the area and while using the Internet at school, pupils should, where possible, be supervised.

Posture - ergonomics

The University of the West of England has provided guidance on safe computer use to ensure that computers are used with a correct posture by ensuring that the chair, keyboard, screen and mouse are properly set up and positioned.

Back problems

Many computer users suffer serious back problems. This is probably due to a poor posture or an awkward position while sitting at a computer.

Solutions

- ✓ A fully adjustable chair should avoid poor posture.
- ✓ Footrests can reduce these problems.
- ✓ Screens should tilt and turn to a position that avoids awkward movements.

Interactive whiteboards and projectors

All interactive whiteboards and other data projectors, if misused, have the potential to cause eye injury, particularly if children stand in front of the beam to give presentations. Simple guidelines should be provided to ensure that:

- ✓ no one should stare directly into the beam of the projector
- ✓ when entering the beam, users should not look towards the audience for more than a few seconds
- ✓ users keep their backs to the projector beam when standing in it
- ✓ children are supervised at all times when a projector is being used

Photosensitive epilepsy

Using a computer is unlikely to be a problem for people with photosensitive epilepsy as the screen flicker is higher than the rate that triggers epilepsy. However, to make sure that any possible risk is kept to an absolute minimum, it is important to consider both the type of software and the display screen.

Epilepsy Action(external link opens in a new window / tab) offers more detailed advice.

Wireless Local Area Networks (WLAN)

The former Health Protection Agency (now Public Health England) advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment.

Guidance on WiFi radio waves and health was published on 1 November 2013 by Public Health England, an executive agency of the Department of Health in the UK, and may be accessed on the Public Health England website(external link opens in a new window / tab).

Eyestrain

Eyes can become strained after staring at a computer screen for a long time, particularly if working in bad light, in glare or with a flickering screen.

Solutions

- ✓ Take regular breaks - do not work for more than one hour without a break.
- ✓ Lighting must be suitable and blinds fitted to windows to reduce glare.

Repetitive Strain Injury (RSI)

Repetitive Strain Injury (RSI) is damage to the fingers, wrists and other parts of the body due to repeated movements over a long period of time.

Solution

- ✓ To prevent RSI, make sure your posture is correct, use wrist rests and have a five-minute break from typing every hour.

APPENDIX 1

Acts of Parliament relevant to e-safety in schools

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 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.)

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 (eg. using someone else's password to access files).
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (eg caused by viruses or denial of service attacks). UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgment. It comes about when an individual expresses an idea in a tangible form. 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.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Counter-Terrorism and Security Act 2015 (section 26)

The prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)

It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years imprisonment.

Data Protection Act 1998 (GDPR from May 2018)

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and data users must comply with important data protection principles when handling personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to cyber-bullying/bullying:

Heads have the power 'to such an extent as is reasonable' to regulate the conduct of pupils off-site. School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) 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. This can include racist, xenophobic and homophobic comments, messages etc.

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.

This also includes incidents of racism, xenophobia and homophobia.

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.

Racial and Religious Hatred Act 2006

This Act makes 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.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes 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.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (eg 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.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. 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). This can include images taken by and distributed by the child themselves (often referred to as 'sexting'). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming 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. Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

APPENDIX 2

Useful organisations/support services for reporting e-safety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

On-line content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Scams

If you have been 'scammed, ripped off or conned' you can report to *Action Fraud* on 0300 123 2040 or http://www.actionfraud.police.uk. This service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

Getting help/advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.

Getting help/advice: for parents

- If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through ParentPort at www.parentport.org.uk. Click on 'Make a Complaint' and ParentPort will take you straight to the right place to complain to.
- Family Lives: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk
- Kidscape: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 5pm, Mondays and Tuesdays on 0207 823 5430 www.kidscape.org.uk.
- Childnet International Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young people to deal with them'. Contact details are: www.childnet.com phone 020 7639 6967, email info@childnet.com.
- UK council for child internet safety (UKCCIS) has practical guides to help parents and others with internet safety www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.
- Thinkuknow has a section for parents which offers advice on protecting children from abuse online offered by the National Crime Agency's CEOP Command www.thinkuknow.co.uk/parents.

Getting help/advice: for teachers

DFE has a telephone helpline (0207 340 7264) and an email address (counter.extremism@education.gsi.gov.uk) to enable teachers to raise concerns or questions directly with them.

Getting help/advice: for professionals working with children

Professionals online safety helpline: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with on-line safety issues www.saferinternet.org.uk.

The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0344 381 4772 (calls on this number are charged at local call rate)