WIDNES ACADEMY WEST BANK

E-Safety POLICY

Recommended by	K Highcock
Approved by	Governing Body
Approval Date	22.10.15
Version Number	1.4
Review Date	September 2018

CHANGE RECORD FORM

Version	Date of change	Date of release	Changed by	Reason for change
1.3	22.10.15		K Highcock	Policy review in the light of changes in legislation
1.4	8.12.16	15.12.16	K Highcock/Anna Myles	Review and update due to ICT provider change. Approved at LGB meeting
1.5	30.6.17	14.7.17	K Highcock	Update to include statement relating to remote access to SIMS system

Introduction

ICT in the 21st Century 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. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

We understand the responsibility to educate our pupils on eSafety 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. Online safety is an area that is constantly evolving and as such this policy will be reviewed at least annually or more regularly in the light of any significant new developments.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

Governing Body

The Governing Body is accountable for ensuring that our school has effective policies and procedures in place; as such they will;

- Review this policy at least annually or more regularly in the light of any significant new developments in the use of the technologies; new threats to e-safety or incidents

that have taken place or if Central Government change the orders or guidance in any way.

- Ensure as and where appropriate, e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
- Keep up to date with emerging risks and threats through technology use
- Receive regular updates from the Principal in regards to training, identified risks and any incidents

Principal

Reporting to the Governing Body, the Principal has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-safety officer, as indicated below.

The Principal will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient i.e. pupils, all staff, senior leadership team, governing Body and parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- All data regarding pupils and staff, financial information and any information classified as confidential (including all data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Pupil/teacher/any school confidential data can only be taken out of school or accessed remotely away from school when authorised by the Principal.

E-Safety officer

The day-to-day duty of e-safety officer is devolved to Miss Anna Myles. All members of the school community have been made aware of who holds this post. The e-safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise herself with the latest research and available resources for school and home use through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal and the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or home.
- Meet regularly with the schools e-safety officers to discuss upcoming issues and projects.
- Liaise with the Local Authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical support
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate for viewing.

All Staff

All staff are to ensure that;

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Principal.
- They have read, understood and signed the Staff Acceptable Use Agreement.
- E-safety activities and awareness are incorporated within curriculum areas.
- The e-safety policy is introduced to pupils at the start of each school year.
- E-safety posters are prominently displayed
- In lessons where internet use is pre-planned, pupils are 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.
- Any e-safety incident is reported to the e-safety officer (and an e-safety incident report is made) or in her absence the Principal. If you are unsure the matter is to be raised with the e-safety officer or the Principal to make a decision.
- Any inappropriate use of the school's virtual learning platform (DBPrimary) is reported to the e-safety officer.
- The reporting flowcharts contained within this e-safety policy are understood.
- Pupil/teacher/any school confidential data is only be taken out of school or accessed remotely away from school when authorised by the Principal.

Safeguarding Designated Person

Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding 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

The Prevent Duty Guidance

Under duties imposed within the Prevent Duty Guidance 2015 as part of the Counter-Terrorism and Security Act 2015, Widnes Academy will ensure that situations are suitably risk assessed, that they will work in partnership with other agencies, that all staff are suitably trained and that IT policies will ensure that children and young people are safe from terrorist and extremist material when accessing the internet in school.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents and carers play the most important role in the development of their children; as such the school will endeavour to ensure that parents and carers have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, workshops and newsletters the school keep parents and carers up to date with new and emerging e-safety risks and will seek to involve parents and carers in strategies to ensure pupils keep themselves safe.

Parents and carers must also understand the schools needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign both the Parent and Pupil Acceptable Use agreement before any access can be granted to school ICT equipment or services.

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

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with an individual network log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Principal
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system and Virtual Learning Platform (DBPrimary), 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.
- All users have an obligation to protect security, confidentiality and integrity of all information.
- In our school, all ICT password policies are the responsibility of the Principal and all staff and pupils are expected to comply with the policies at all times.

Data Security

Staff are aware of their responsibility when accessing school data. They must not;

- allow others to view the data
- store data on an unencrypted memory stick or use it to store child related information
- store child related information on any device other than on a school device or network
- edit the data unless specifically requested to do so by the Principal.

Managing the Internet

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. All use of the Internet is logged through a locally installed Smoothwall Web Filtering Appliance and the logs are only accessible to appropriate staff members which could be randomly monitored. Whenever any inappropriate use is detected, it will be followed up by **the** Support Team at Wade Deacon through its eSafety responsibilities.

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

Widnes Academy has a monitoring solution procured for and managed by Wade Deacon through Multi Academy Trust services where web-based activity is monitored and recorded.

School internet access is controlled through the Smoothwall web filtering service.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission

Social Networking

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative 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 pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school. It is also noted that the age of the children would suggest that they are too young to sign up to social networking sites but may have access to them. Therefore all the advice and teaching is given in context of being SMART on line.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils 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.
- Pupils 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).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school or if they see anything that makes them feel uncomfortable.

The following social media services are permitted for use within Widnes Academy:

Twitter – used by school as a broadcast service
Facebook – used by school as a broadcast service

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.

- Pupils are not allowed to bring personal mobile devices/phones to school unless by prior agreement with the Principal/class teacher. In these instances pupils must hand their phones to the class teacher who will keep the device during the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages 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.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text 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 Ipads and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- 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.
- 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 pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- 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.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Children use a class/group email address.
- The forwarding of chain letters this includes jokes and funny statements. is not permitted in school.

- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Scheme of Work.

Safe Use of Images - Taking of Images and Film

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

The following guidelines must also be observed:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g on social networking sites.
- In accordance with guidance from the Information Commissioners Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect and protect everyone's privacy, these images should not be published/ made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- 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.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

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

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils 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 pupils within the confines of the school network/ Learning Platform.
- Each member of staff or the ICT Co-ordinator has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Principal. Incidents should be logged.

Incidents

Any e-safety incident is to be brought to the immediate attention of the e-safety Officer or in her absence the Principal. The e-safety Officer will assist staff in taking the appropriate action to deal with the incident and fill out an incident log.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Principal/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Principal.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

This policy will be reviewed annually 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.

The next review date will be September 2016.

School – Widnes Academy West Bank
Acceptable Use Agreement: Staff, Governors and Visitors
Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.
Any concerns or clarification should be discussed with the school eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal 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 pupils and staff 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 pupils.
- 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. Personal data can only be taken out of school or accessed remotely when authorised by the Principal.
- I will not install any hardware of software without permission of the Principal.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline 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 Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal.
- 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.
- I will support and promote the school's e-Safety policy and help pupils 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 ICT throughout the school

Signature …… Date …….

Full Name ……..(printed)

School…….

Job title . . . . . .

School – Widnes Academy West Bank
Primary Pupil Acceptable Use
Agreement / eSafety Rules
(From Year Two)

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

School – Widnes Academy West Bank

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Angela Harrison, ICT Co-ordinator

✂---

Parent/ carer signature
We have discussed this and ……………………………………........(child name) agrees to follow the eSafety rules and to support the safe use of ICT Widnes Academy West Bank.

Parent/ Carer Signature …………………………………………………….

Class …………………………………. Date ………………………………

Acceptable Use Agreement:

Dear Parent/ Carer

ICT including the internet, learning platforms, email and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mrs Angela Harrison, school eSafety coordinator.

Please return the bottom section of this form to school for filing.

✂- -

Pupil and Parent/ carer signature
We have discussed this document and …………………………………….........(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Widnes Academy West Bank.

Parent/Carer Signature ………………………………………………….

Pupil Signature……………………………………………………………….

Form ………………………………… Date ………………………………

School Incident Log

'School name' eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

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

Current Legislation

Acts relating to monitoring of email

Users of this list should note that legislation is open to change and should always verify that the references and versions given or linked are up to date before relying on them.

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however,

permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

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

Other Acts relating to eSafety

The Prevent Duty Guidance 2015 as part of the Counter-Terrorism and Security Act 2015

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.

The Education and Inspection Act 2006
Empowers headteachers, to such an extent as is reasonable to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspection Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

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.

Freedom of Information Action 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests they have to follow a number of set procedures.

Trade Marks Act 1994
This provides protection for Registered Trade Marks which can be any symbol (words, shapes or images) that are associated with a particular set of good or services. Registered Trade Marks must not be used without permission. This can also arise from using a m ark that is similar to an existing mark.

Criminal Justice and Public Order Act 1994
This defines a criminal offence of intentional harassment which covers all forms of harassment including sexual. A person is guilty of an offence if with intent to cause a person harassment, alarm or distress they:

- Use threatening, abusive or insulting words or behaviour or disorderly behaviour or
- Display any writing, sign or other visible representation which is threatening, abusive or insulting thereby causing that or another person harassment, alarm or distress.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Telecommunications Act 1984
It is an offence to send an message or other matter that is grossly offensive or of an indecent obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Widnes Academy West Bank

Adopted by the Governing Body …….

Item Number in Minute of Meeting: …….

Appendix

E-Safety Incident Log

Date and Time	Name of Pupil/Staff Member	Male/Female	Room/Device number	Details of Incident	Actions and Reasons