# E- Safety Policy

## Mission Statement

Our mission statement acknowledges that each person is made in the image and likeness of God and therefore worthy of respect, dignity and protection from that which may harm their physical or emotional well-being. We strive to promote "a warm atmosphere, full of caring relationships." Our priority is the welfare of our girls and we are committed to the highest standards in protecting and safeguarding the girls entrusted to our care at all times.

## What is an E-safety Policy?

- The school e-safety policy aims to create an environment where pupils, staff,
- parents, governors and the wider school community work together to inform each other of ways to use the internet responsibly, safely and positively.
- Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

## Introduction

**Ofsted statements:**

**Ofsted have defined E-safety thus:**

- 'In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.'

**E-safety will be inspected in relation to the following areas:**

- "The behaviour and safety of pupils at the school.
- The quality of leadership in, and management of, the school"

**Ofsted have identified three areas of e-safety risk in relation to pupils:**

- "Being exposed to illegal, inappropriate or harmful material.
- Being subjected to harmful online interaction with other users.
- Personal online behaviour that increases the likelihood of, or causes, harm."

**An outstanding school will demonstrate that:**

- “All groups of pupils feel safe at school and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to e-safety.”

**Ofsted will examine how the school:**

- Audits the training needs of all staff and provides training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Works closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Uses pupils’ and families’ views more often to develop e-safety strategies
- Manages the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- Provides an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- Works with partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- Systematically reviews and develops e-safety procedures, including training, to ensure that they have a positive impact on pupils’ knowledge and understanding.
- Ensure pupils are aware of e-safety reporting procedures in school.

**Key features of good and outstanding practice:**

- All staff understand E-safety issues. E-safety is a school priority. The school has, or is working towards an E-safety Mark. Training in E-safety is audited and provided to all staff. A number of members of staff will be receiving accredited E-safety training ( ICT support, DSLs and named safeguarding Governor) Pupils, parents, wider school community stakeholders and governors all contribute to build a fluid and constantly evolving E-safety policy.
- Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of e-safety. All staff, parents, pupils, and governors know how to report an E-safety incident.
- The school uses recognised and accredited providers for internet provision and filtering.
- The E-safety policy is closely integrated with relevant policies and procedures, including child protection, safeguarding, acceptable use, anti-bullying and behaviour.

• The acceptable use policy agreements have been developed with, signed by, and agreed to by all users of school IT systems
– pupils, parents, staff, governors and visitors.
• The school promotes a real world, responsible and positive outlook towards Digital Literacy and e-safety aimed at preparing pupils for expected standards of behaviour in adult life and the workplace.

**E-safety Policy Scope**

• The school E-safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related internet and computer systems internally and externally.

• The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and internet usage both on and off the school site. This will include imposing rewards and sanctions for behaviour and penalties for inappropriate behaviour – as defined as regulation of student behaviour under the Education and Inspections Act 2006.

‘In Loco Parentis’ provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment, malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

**The E-safety policy covers the use of:**

• School based ICT systems and equipment.
• School based intranet and networking.
• School related external internet, including but not exclusively, firefly VLE, e-learning platforms, blogs, social media websites.
• External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
• School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones.
• Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or internet facilities.
• Mobile phones, devices and laptops when used on the school site.

**Reviewing and evaluating E-safety and ensuring good practice**
**Monitoring the E-safety policy:**

The e-safety policy will be actively monitored and evaluated by an E-safety group. This committee will comprise:

• Designated Safeguarding Leads: Dawn Casserly, Anne-Marie Canavan, Sarah Liddall
• Link DSL for E-Safety: Anne-Marie Canavan
• Strategic ICT Network Manager: James Wilson
• Senior Leadership Team
• Designated Teaching Staff
• Designated Support Staff
• E-safety Governor: Alinka Starzewka
• In the event of an E-safety incident, the following people will be informed within school and in external agencies and stakeholder organisations: Dawn Casserly, Anne-Marie Canavan, James Wilson, appropriate head of year. Outcomes will be fed back to staff as appropriate.

**The E-safety calendar**
**E-safety policy review and evaluation schedule:**

• The E-safety policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year.
• Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable internet use policy or other in the light of e-safety incidents.
- New guidance by government / LA / safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- E-safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police.

• The E-safety policy review will be documented in the school development plan and school self- evaluation and improvement profiling.
• The school will draw up an E-safety calendar detailing training, meetings, reviews, evaluations, teaching and learning provision, parental involvement, wider community involvement and governor involvement over an academic year. Regular use will be made of staff, parent and pupil e-safety audits, and pupil AfL questionnaires to inform E-safety learning, staff training requirements, gauge the impact and effectiveness of the E-safety provision and determine future E-safety targets.
• The E-safety calendar needs to include a schedule of events, which feed into the E-safety development or action plan. As well as an audit of parental E-safety knowledge, it is worth carrying out parental satisfaction polls regularly.
• It is good practice to include parents, older pupils and peer-group pupils in E-safety presentations – to provide illustrative examples of E-safety issues.
• Evaluation, review, revision and training should be ongoing activities, linked into points in the yearly E-safety calendar.
• LA – child protection, and safeguarding meetings should be referenced in the E-safety calendar.

**Policy review schedule:**
• The e-safety policy will be monitored annually.
• The E-safety policy will be reviewed and evaluated promptly in the light of serious E-safety incidents.
• The E-safety policy will be reviewed and evaluated promptly in the light of important changes to legislation or government guidance related to E-safety.
• The Governing Body will receive a report on the progress, evaluation, impact and effectiveness of the E-safety policy annually. This report will include suitably redacted accounts and statistics of E-safety incidents and how these have been resolved, and counter measures implemented.
• The E-safety group and E-safety Link DSL will include in reports evaluations of the impact of the E-safety policy by evidencing – for example - E-safety incidents, written reports, statistics of filtering breaches, logs of internet and network traffic activity, AfL teaching questionnaires and E-safety audits of staff, support staff, parents, governors and other stakeholders, ParentView and Ofsted questionnaire results.

## Who does E-safety affect, who is responsible for E-safety and what are their roles?

### School Management and E-safety

• School senior leadership is responsible for determining, evaluating and reviewing E-safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and governors of internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

- E-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and internet developments, current government guidance and school related E-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships.
- E-safety provision is always designed to encourage positive behaviours and practical real world strategies for all members of the school and wider school community.
- Management is encouraged to be aspirational and innovative in developing strategies for E-safety provision which will deliver measurable success via a calendar of E-safety provision and clearly state E-safety targets with success criteria on the school development plan.

**Evidence base:**

- School development plan and school improvement plan
- E-safety calendar
- Minutes from E-safety related meetings with staff, SLT, parents association, governors and wider school community stakeholders
- Regularly updated E-safety policy, child protection policy and logged and evaluated E-safety incidents.
- Staff inset provision audit and record.

**The school E-safety Link DSL:**

- The school has a designated E-safety officer Anne-Marie Canavan who reports to the SLT and Governors and coordinates E-safety provision across the school and wider school community. The group liaises with SLT, the other school Designated Safeguarding Leads and other senior managers as required.
- The school E-safety designated DSL has a specific job description and person specification detailing the role, remit, qualifications and qualities required for the post. This specification is updated according to the school cycle for reviewing job descriptions.
- The school’s E-safety designated DSL leads the school e-safety group which includes representatives of the school SLT, teaching and support staff, governors, parents, pupils and the wider school community including relevant local stakeholders.
- The school E-safety group meets regularly at intervals defined in the school’s E-safety calendar.
- The school E-safety designated lead and Strategic ICT Network Manager are responsible for E-safety issues on a day to day basis and also liaises with LA contacts, filtering and website providers.
- The school E-safety designated DSL maintains a log of submitted E-safety reports and incidents.
- The school E-safety designated DSL audits and assesses inset requirements for staff, support staff and governor E-safety training, and ensures that all staff are aware of their responsibilities and the school’s E-safety procedures. The school E-

Safety designated DSL is also the first port of call for staff requiring advice on E-safety matters.

- Although all staff are responsible for upholding the school E-safety policy and safer internet practice, the e-safety designated DSL, the other DSLS and ICT support are responsible for monitoring internet usage by pupils and staff on school devices.
- The E-safety designated DSL is responsible for promoting best practice in E-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.

**Governors' responsibility for E-safety:**

- At least one Governor is responsible for E-safety, and the school E-safety designated DSL will liaise directly with the Governor with regard to reports on E-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.
- To provide and evidence a link between the school; governors and parents, it is suggested that a parent-governor be appointed to this role.
- An audit of Governor IT competence, relevant outside experience and qualifications is advisable to identify training needs and create a schedule and development plan. It is essential that Governors tasked with overseeing and monitoring E-safety have demonstrable experience, skills or qualifications to match the role. The E-safety Officer/coordinator will be responsible for auditing Governor E-safety training and inset requirements.

**ICT support staff and external contractors:**

- Internal ICT support staff are responsible for maintaining the school's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Maintain and enforce the school's password policy and monitor and maintain the internet filtering.
- Where contractors have access to sensitive school information and material covered by the Data Protection Act, for example on a VLE, school website or email provision, the contractor should also be DBS checked.

**Teaching and teaching support staff:**

- Teaching and teaching support staff need to ensure that they are aware of the current school E-safety policy, practices and associated procedures for reporting E-safety incidents.
- Teaching and teaching support staff will be provided with E-safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to internet and computer use in school.
- All staff need to follow the school's social media policy, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.

• All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
• Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
• Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

**Designated Safeguarding Lead :**
• The DSLs to be trained in specific E-safety issues. Accredited training with reference to child protection issues online is advised – for example a CEOP accredited course or a Cyber mentor course.
• The DSLs needs to be able to differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
• Possible scenarios might include:

- Allegations against members of staff.
- Computer crime – for example hacking of school systems.
- Allegations or evidence of 'grooming'.
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
- Extremist behaviour as indicated by the PREVENT policy
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

**Pupils:**
• Are required to use school internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
• Pupils need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.
• Pupils need to be aware that school Acceptable Use Policies cover all computer, internet and device usage in school, including the use of personal items such as phones.
• Pupils need to be aware that their internet use out of school on social networking sites such as Facebook is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation or illegal activities.

**Parents and Guardians:**
• It is hoped that parents and guardians will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home.
• The school expects parents and guardians to sign the school's Acceptable Use Polices, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.

- The school will provide opportunities to educate parents with regard to E-safety.

**Other users:**

- Other users such as school visitors, or wider school community stakeholders or external contractors should be expected to agree to a visitor’s AUP document or a tailored AUP document specific to their level of access and usage.
- External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

**How will the school provide E-safety education?**
**Possible curriculum opportunities:**

- E-safety as an ICT teaching unit; how to judge the validity of website information, how to remove cyber bullying, computer usage and the law, how to spot and remove viruses, why copyright is important.
- E-safety as a PSHE teaching unit: how to deal with cyber bullying, how to report cyber bullying, the social effects of spending too much time online.
- E-safety as part of pastoral care – form time activities, assemblies, year group presentations, tutorial opportunities.
- E-safety events – such as Safer Internet Day and Anti Bullying Week.

**Parents – information, presentation, collaborative meetings and events:**
**Possible information dissemination opportunities:**

- E-safety information directly delivered to parents: newsletters, mobile text, school website and VLE.
- Parents Evenings, open days, transition evenings, or other events to take advantage of occasions when there are large numbers of parents in school.

**Staff – inset and training:**
**Possible training and information dissemination opportunities:**

- E-safety information directly delivered to staff: newsletters, emails, website or VLE.
- A planned calendar programme of E-safety training opportunities to be made available for staff, including on site inset, whole staff training, online training opportunities (for example E-safety Support courses), external CPD courses, accredited CPD courses, (for example Cyber mentors or CEOP)
- The E-safety policy will be updated and evaluated by staff at the beginning of each academic year and timetabled into the INSET day schedule.
- The e-safety designated DSL should be the first port of call for staff requiring e-safety advice.

**Governors – training:**
**Possible training and information dissemination opportunities:**

- E-safety information directly delivered to governors: letters, newsletters, emails and website.
- Open days, or other events to take advantage of occasions when there are large numbers of visitors in school.

• Governors should also be provided access to staff inset training, or specific governor training provided externally (for example by the LA, NAACE online or the National Governors Association.)

**ICT Support Staff, filtering and monitoring:**
**Possible training and information dissemination opportunities:**

• E-safety information directly delivered to support staff: emails or VLE.

• Open days, or other events to take advantage of occasions when there are large numbers of visitors in school.

• Support staff should also be provided access to staff inset training.

• IT support staff and should ensure that bought in hardware and software solutions feature built in training provision (where applicable).

• Support staff and contractors need to be DBS checked and agree and sign the school's e-safety AUP.

• IT technical support staff and network managers should have relevant industry experience, training and qualifications.

**Particular behaviour which will be highlighted might include:**

• Explaining why harmful or abusive images on the internet might be inappropriate or illegal.

• Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.

• Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.

• Teaching why certain behaviour on the internet can post an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practises such as grooming can develop.

• Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.

• Teaching pupils to assess the quality of information retrieved from the internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.

• Informing pupils and staff of copyright and plagiarism infringement laws, and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally.

• Encouraging responsible and effective digital literacy skills which extend beyond school and into the workplace.

• The medical and social effects of spending too much time on the internet, games consoles or computers.

**E-safety in practice - Guidance for Senior Leadership Team**
**Systems:**

• School computer systems should be firstly fit for purpose, and secondly customised to ensure e-safety. For pupil machines, the primary purpose is to ensure the configuration of school computers, networks and file-serving is designed to meet the teaching and learning requirements of the school. E-safety must then be fully implemented without sacrificing the teaching and learning requirements and functionality. Similarly, for staff machines, the primary purpose when considering network design is how best to meet the needs of staff use and school administration. E-safety requirements must be designed with this in mind.

• Network managers should always ensure that school, LA, DFE, ICO and Data Protection guidelines with regard to E-safety are met and implemented.

• Network managers need to carry out regular audits and evaluations of the school IT network and should maintain an ongoing development plan for IT provision.

• The key E-safety aims with regard to computer systems, access, file-serving and networking are to create a system which can log, track and evidence e-safety events, and provide data to enable accurate evaluation and improvements to be made. This needs to be borne in mind when justifying any decision regarding E-safety and network design and implementation.

• Network managers need to create a system where every login, data transaction, or other activity can be logged, traced to a particular user and monitored in the event of abuse.

• All physical network hardware should be should be secured to prevent unauthorised or untraceable network access.

**Filtering:**

• Your filtering provider should be the first port of call for advice regarding filtering. It is best practice if they provide the basis for a filtering policy, based precisely on the system and settings in operation for the school. If generic or inaccurate policies are used, a misleading impression of the filtering process and logging capability can be created. It is not advisable to purchase a package or subscribe to an external contractor if they are unable to provide this information and in the form the school requires. Detailed polices will be provided by the LA and should be adopted without any significant alteration.

• The school’s internet service must be provided by a fully accredited ISP. Accredited filtering should be used. The school must be able to differentiate the levels of filtering based on pupil age, maturity, responsibility; and staff use. The filtering reports and logs should be examined daily, and if possible there should be a facility to monitor ‘on the fly’. Classroom management systems should be utilised by teaching staff to monitor all pupils’ screens on one staff screen or IWB. Any alterations to the filtering protocol are authorised, recorded and reasons provided. Any filtering ‘incidents’ are examined and action is taken and recorded to prevent a reoccurrence.

• Filtering and monitoring needs to reflect real life rather than being a ‘lock down’ system. If locked down, or white-list only, the school risks simply transferring E-safety problems incidents elsewhere – for example to mobile phones, or home usage. The problem isn’t being dealt with and good behaviours are not being taught. Pupils need to be taught positive responsible behaviour to carry forward into the workplace.

**Providers include:**

http://www.smoothwall.net/solutions/education/
http://www.rm.com/products/school-broadband

**Monitoring:**

• Your installed monitoring package (software or hardware) manufacturer or provider should be your first port of call regarding capabilities and procedures. It is best practice to use a monitoring solution which includes an exemplar procedure for monitoring and logging activity. Generic policies are not advised since no two monitoring packages are the same. To achieve the school's precise E-safety aims may require the use of more than one monitoring and logging package.

**Packages include:**
http://www.rm.com/products/rm-community-connect
http://www.rm.com/products/rm-tutor
http://www.forensicsoftware.co.uk/education/index.aspx
http://learnpad.com/uk/classview/

**Network security:**
**Passwords:**
• The use of network profiles which require the user to input a username and password is one way to enable the network manager to log network and internet activity specific to a user, in order to fulfil E-safety requirements.
• If the school uses this method, it is essential to use "strong" passwords and enforce an automated password expiry for a prescribed interval – for example – twice-termly.
• There are flaws with this approach which the network manager will need to consider carefully. Firstly, passwords can be shared. Secondly, pupils might work in pairs or small groups, thirdly computers can be left logged on and as a result another user could cause an E-safety incident which could be incorrectly attributed to the wrong person.
• Furthermore, with younger children and older machines, requiring all pupils to switch machines on and log in prior to the teacher beginning the lesson can take a significant amount of time – in some cases up to seven minutes – which is unacceptable for teaching and learning. Best practise for teaching and learning is to create a situation where all technology is "ready to go" prior to the students entering the room. It is not always possible to achieve this with network wide profile logins.
• The school password policy needs to be configured with the assistance of the Network Manager to ensure:

- A password history is kept so that old passwords are not re-used.
- Passwords expire after a set number of days – and not in the holidays - otherwise the first day of term is chaos.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords must meet complexity requirements – ie they need to be 'strong' passwords, for example using upper and lower case letters, numbers and symbols.
- Passwords should be stored using non-reversible encryption – in other words there should not be a great big text file with all the passwords for pupils to find on the network – passwords should be encrypted.

• Pupils and staff should be encouraged to change passwords – for all important accounts, and not just school profiles –regularly. A 'change your password' day at least once a term is one possible idea.
• Backups should be made to encrypted fileservers or partitions – to prevent an individual walking away with an entire school network on a portable hard-drive. If cloud services are used, the TOS of the cloud host need to be scrutinised extremely carefully given the ICO requirements for storage of "personal data". Generally, cloud backup services are not advised for personal data.

**Policy guidance for handling personal data, dealing with freedom of information requests, and complying with privacy regulations pertaining to website data:**

All of these areas are regulated by the Information Commissioner (ICO), and every UK organisation has to comply with the responsibilities and obligations as defined by the ICO. Schools are no different to any other organisation in this regard. The ICO guidance on how to comply with these obligations is updated regularly. Therefore, it is best practice to refer directly to this guidance in these areas, rather than formulate a policy based on guidance which may well be updated prior to the next policy review date.

When disposing of computer equipment, schools needs to ensure all data, including personal data is wiped, not deleted from storage. A useful guide can be found here: http://www.getsafeonline.org/protecting-your-computer/safe-computer-disposal/. If the school is offered second hand or reconditioned machines by parents or well-wishers, very careful consideration needs to be given as to whether to accept. Any storage needs to be wiped with the above guide before being integrated into school use.

**Use of IT facilities for curriculum teaching and learning:**

Use of the internet and IT facilities should be clearly planned prior to the activity. Students should be trusted to be responsible when researching the internet, but the filtering software needs to be flexible enough to allow teaching staff to manually filter by category as well as specific site depending on the age and maturity of the students.

**Use of images and videos and advice on creating a photo permissions agreement:**

- In terms of E-safety, schools must ensure images and videos or pupils, staff, pupil's work and any other personally identifying material must be used, stored, archived, and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools, National College for Teaching & Leadership guidelines for teacher and the schools AUP.
- The ICO publishes comprehensive advice for schools, parents and pupils with regard to the Data Protection Act. This advice helps dispel many of the urban myths.
- Guide for schools: http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx
- Advice re taking photos in schools: http://www.ico.gov.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_application/TAKING_PHOTOS_V3.ashx
- Advice for pupils: http://www.ico.gov.uk/Youth.aspx
- Parents taking photographs of children at sports day and play productions etc – the Data Protection Act does not feature a bar to parents taking images of their children, or indeed any other children, at school events. There are no laws preventing the taking of photographs in public spaces, and no permission is required to take photographs in public places. However, on private property, the permission of the property owner, or in the case of a school the proprietor or the person with this delegated responsibility (normally the Head teacher) is required.
- http://content.met.police.uk/Site/photographyadvice
- If the school does want to restrict the taking of photographs on the school site, it should not invoke the "Data Protection Act." Instead, if the school wants to prevent

the 'publication' of photographs (or videos) taken on the school site (for example on the internet), and limit the use of photographs, for example, to home photo albums, then there is provision in law to achieve this. (http://www.legislation.gov.uk/ukpga/1988/48/section/85) The school needs to assert that they are allowing the photography of the school event by the invited parent providing the parent "agrees to use the image only for private and domestic purposes." This refers to a right to limited right of privacy determined in the Copyright Designs and Patents Act 1988 to prevent the photographer in such a situation exhibiting the work in public; normally used to prevent the publication wedding and party images. Enforcing a breach in law might well prove difficult, although it does provide the school with means to remove images published by parents or pupils on the internet by claiming copyright infringement under http://www.legislation.gov.uk/ukpga/1988/48/section/85. This would, for example, facilitate a straightforward removal process for Facebook, Twitter and most websites.

- School photography policies should therefore refer only to instances where the school can control the taking of photographs. Statements such as "photography at sports matches is prohibited", "photographs of children taken at events will not include names" or "parents must not take photographs of children which are not their own," are not enforceable, and unwise. Schools, for example, should not make claims regarding the publication of names of pupils which they might not be able to control. For example, if a school asserts that names of pupils will never be published in a way which might identify the pupils, and then a newspaper takes a photograph, asks the pupils their names and publishes – the school will be liable for complaints despite not being responsible for the publication. In such cases, statements should be limited and specific to only what a school can reasonably control or be held responsible for.
- Regarding photo permission, an "all or nothing" option is by far the safest. Parents should be able whether to decide or not to allow the school permission to take photographs of their child at events. Any middle ground options simply increase the chances of an unfortunate breach of the policy. Similarly, the school should assert that "All reasonable steps will be taken to prevent identifying information being included with photographs taken on the school site," since the school simply doesn't reasonably have the means to control any publication off the school site by other schools, event organisers, the press, or members of the public. The schools can suggest that "All local press and media organisations have been informed that X school does not wish identifying information to be published with photographs of its pupils taken at local and regional events," and then the school has taken reasonable steps, and the onus is on the press.
- It is always worth including a statement on travel permission letters for events to the effect that "Photographs of pupils may be taken by the event organisers and media. The school is not in control of the publication of such images and parents will need to consider this when granting permission for your child to attend this event."
- http://en.wikipedia.org/wiki/Photography_and_the_law

**Photography permission discrimination at events:**

- Some events might already include specific and required permission slips for parents to sign regarding the taking of and use of images – for example BBC News Report or the Times Spelling Bee. The school needs to make it clear to parents that the 'requirement' for parents to sign such forms to "allow" participation is the requirement of the organiser, and not the school. It is essential that the school is not seen to discriminate participation at events on the grounds of permission to take photographs of pupils. Such discrimination must be clearly attributed to the event organiser.

• Under the Data Protection Act and ICO guidance schools can create and use images for school, for official school use in education activities which form the normal running of the school. For example, student photo-id passes and classroom room display come under this provision. Schools can also take photographs for websites, newsletters and to provide to media, and the ICO advises schools request permission and inform the parents to make them aware this is taking place, and of the context.

• School should store images which are defined as "personal data", securely, in line with the terms of the Data Protection Act. Secure storage can be defined as an area on a school network which requires a secure username and password to access, or an encrypted data storage device, or a cloud storage solution access by a username and password over an SSL (encrypted) connection.

• If teachers use their own cameras, the images should be stored securely on a school computer, network area or cloud storage solution. Teachers should not store copies of such images on their own computers or storage devices, and images should be deleted from staff cameras or camera storage devices once transferred to a school secure storage. Some schools fulfil this requirement by using a 'school camera'. However, a more efficient and cheaper solution is to ask staff to use "school camera storage cards", allowing staff to use their own camera.

• If schools keep an archive of images, for example school photographs, displays, or events, it is advisable to use a professional management system such as Adobe Lightroom, which can be stored on a secure network fileserver. Alternatively, cloud solutions can be used, but these need to be operated on secure connections – for example Amazon S3. Public access, non-secure services such as Flickr and Picassa are unsuitable for storing images classed as "personal data" under the DPA, but are fine for images where permission has been granted for school promotional and/or media use.

**Data Protection and E-safety:**

• The Data Protection Act is relevant to E-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

• In particular, Ofsted are likely to examine how the school ensures information is kept secure in school, and particularly if it leaves the school site, or if there is a potential for gaps in security when transferring material to and from the school site.

• Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

• Personal data should only be stored on secure devices. In other words, only computers, servers, file-servers, cloud space or devices which require a user name and password to access the information. Furthermore, web based, extranet, E-learning or cloud services which include personal information need to run over an https:// protocol – ie an SSL secure encrypted connection.

• Secure accounts need to be logged off after use to prevent unauthorised access. It is good practice to set accounts which can access personal data to automatically lock after a defined period of inactivity – for example 15 minutes.

• Various devices are marketed towards school to fulfil a perceived requirement for 'encryption'. These include encrypted memory sticks and pen drives. Schools need to bear in mind that such devices are sold at a significant mark up to schools, and any memory stick or pen drive can be converted for encrypted use with free software.
•http://www.esecurityplanet.com/views/article.php/3880616/How-to-Encrypt-a-USB-Flash-Drive.htm
• By far the most effective way to safeguard personal data when off the school site it not to transfer personal information outside school systems. There is no real reason why any personal data should need to leave the school site. For example, http://logmein.com offers secure encrypted remote log in access which will work with any school computers or network, allowing staff to access material securely from home – and the personal information never leaves the school site – it is simply viewed remotely. If a particular file is required off site, a member of staff can email the file to themselves, and then access the email, off site, via the school's webmail or staff network login, and the personal material will not have left the secure school system. If the school's Data Protection / e-safety policies are designed to keep all information within secure school systems, the risk of unauthorised access or a breach of Data Protection regulations is minimal.

• **Using Email:**
Pupils need to be made aware that messages are monitored and that the filtering system will detect, for example, inappropriate links, viruses, malware, and profanity.
• If staff email is monitored, the staff need to be made aware of this.
• If the school does not have the facility to monitor and filter email, secure educational webmail portals, such as http://epals.com are recommended for this purpose.

**Personal information on the school website:**
• No material defined as 'personal information' under the Data Protection Act should be used on a public school website.
• Schools need to consider staff privacy issues carefully with regard to publishing staff email addresses, staff lists, photos of staff, staff qualifications and any other personally identifying information. If such information is included on a public website, it is best practise to instruct the web designer to include "noindex", "nofollow" and "noarchive" tags on the staff list webpages to ensure any information or images are not copied onto other websites, including search engines.
• It is better practice to include any information made up of lists of names and/or contact details (for example staff lists or lists pupils names for sports teams) on VLEs which are accessible to the school community, but not the wider public or search engines such as Google.

**What activity is deemed inappropriate:**
The school needs to clearly define which online and network activities are appropriate and which are not. It is essential that the inappropriate activities are discussed and the reasoning behind prohibiting activities due to E-safety are explained to pupils in curriculum and co-curricular activities in order to promote responsible internet use. As far as possible, restrictions need to reflect real life to precipitate a smooth transition to adult life in terms of the law, further education/university expectations, workplaces practices and public sector guidelines.

**How to deal with E-safety incidents – action to take:**
The precise chain of events for reporting an E-safety incident will vary from school to school. Below are some suggestions, based on the nature and severity of the incident.

**If you find illegal material on your network, or log evidence to suggest that illegal material has been accessed**
• If the illegal material image is (or is suspected to be) a:

- Child sexual abuse images hosted anywhere in the world.
- A non-photographic child sexual abuse images hosted in the UK.
- Or a criminally obscene adult content hosted in the UK.

• Report to the IWF - https://www.iwf.org.uk/report. Contact your local police. Follow your school's child protection procedures if a child protection incident is suspected but: do not copy, archive, forward, send or print out the image – leave it in situ, and if in doubt seek advice from the IWF or your local police.

**If there is a child protection issue:**
If there is a child protection issue, your school and/or LA Child Protection policy will apply. It is better practice to refer to other key policies rather than develop potentially confusing and overlapping policy areas.

**If there is illegal material which you are unable to remove which involves Grooming, or suspected child abuse via the internet c**all your local police. Also contact CEOP http://www.ceop.police.uk/safety-centre/ who have an excellent record for removing such material quickly.

**How to deal with e-safety incidents – indicative sanctions for pupils and/or staff:**
**Suggested outcomes for specific incidences – who should be responsible for dealing with, and writing up and incident report?**
To promote positive pupil behaviour it is suggested that there is a demonstrable correlation between procedures and sanctions for pupils, and procedures and sanctions for staff. It also needs to be explained to pupils how the school's determined policy relates to similar scenarios and how they would be dealt with in the workplace.

**Illegal activities:**
• The Headteacher or delegated SLT with responsibility for pupil behaviour will deal with the matter.
• The Police and IWF/CEOP should be contacted. Child Protection procedures take precedence over AUPs if CP is a factor.
• The Network Manager, School IT Support should be contacted to obtain further evidence.

**Going on the internet in lessons or using websites not relevant to the lesson in lesson time:**
• Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.

• Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
• The person will receive a warning.
• The person will receive a sanction, decided by SLT and / or Pastoral staff.

**Bypassing the school’s filtering system:**
• Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: The issue may be raised by SLT to the Head teacher as a disciplinary matter.
• Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the E-safety designated lead. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
• Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
• The School ICT Support should be contacted to obtain further evidence.
• Additionally, parents or guardians will need to be informed.
• The person involved will lose access to the network and/or internet as per the AUP agreement.
• The person will receive a sanction, decided by SLT and / or Pastoral staff.

**Viewing pornographic material:**
• Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the E-safety designated lead. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
• Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
• The Police and IWF should be contacted if indecent material was uploaded or downloaded. CEOP should be contacted if grooming / sexting or unwanted sexual advances were involved.
• The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
• Additionally, parents or guardians will need to be informed.
• The person involved will lose access to the network and/or internet as per the AUP agreement.
• The person will receive a sanction, decided by SLT and / or Pastoral staff.

**Using a mobile phone or other digital device in a lesson (with the exception of sixth form BYOD):**
• Pupil: The phone will be confiscated and parents informed. The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer
• Staff: The issue may be raised by SLT to the Head teacher as a disciplinary matter

The person will receive a warning. The person will receive a sanction, as defined in the AUP policy.

**Using social media (Twitter and Facebook) or email in lesson time:**
- Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer. Staff: The issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person will receive a warning.

**Cyber bullying:**
- Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: The issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- The Police may be contacted.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

**Writing malicious comments about the school or bringing the school name into disrepute – whether in school time or not:**
- Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: The issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.

- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

**Sharing usernames and passwords:**

- Pupil: The class teacher or form tutor will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: The issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- School ICT Support should be contacted to obtain further evidence.
- The person will receive a sanction, decided by SLT and / or Pastoral staff.

**Deleting someone else's work or unauthorised deletion of school files:**

- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- School ICT Support should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or internet as per the AUP agreement.

**Trying to hack or hacking into another person's account, school databases, school website, school emails or online fraud using the school network:**

- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Depending on the severity of the incidence, the http://content.met.police.uk/Site/pceu cybercrime unit, http://www.actionfraud.police.uk/ or local police could be contacted.
- School ICT Support should be contacted to obtain further evidence.
- Additionally, parents or guardians will need to be informed.
- The person involved will lose access to the network and/or internet as per the AUP agreement.

**Copyright infringement of text, software or media:**

- Pupil: A Head of Department or Head of Year or Head of Pastoral Care will deal with the matter and write up an incident report to submit to the e-safety designated lead. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- Pupil: The Head teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter. Staff: the issue may be raised by SLT to the Head teacher as a disciplinary matter.
- School ICT Support should be contacted to obtain further evidence.
- The person will receive a sanction, as defined in the AUP policy.

**E-safety and the Law:**
Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Head teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.)

**Copyright infringement and DMCA:**
If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto site such as Facebook and Twitter.

**Duty of care and ‘in loco parentis’:**
Schools have a ‘duty of care’ to pupils and as such act “in loco parentis.” Under the Children Act 1989, this enables schools to remove personal information, cyber bullying and comments relating to school pupils as if they were the child’s parent. Facebook in particular has provision for using ‘in loco parentis’ when reporting cyber bullying. This is relevant to all schools, but especially to boarding and residential schools.

**Specific school policies to support good practice in e-safety:**
**Acceptable Usage Policy:**

- The school Acceptable Usage Policy covers use by pupils, staff and other adults working in school and also the usage of school related internet technologies such as E-Learning platforms, website, social media and external network logins.
- Acceptable Use policies are tailored for each for pupils; and by category of adult. These policies are signed annually by pupils, staff and other adults working in school.
- The purpose and scope of the E-Learning Policies are explained to those required to sign and agree to them by means of a presentation and opportunity to ask

questions. New pupils will be informed of the scope and purpose of the AUPs as part of induction prior to joining the school, or at the start of their first term. For pupils, this purpose and scope is also explained to parents by means of explanatory notes accompanying the policy to sign, and in presentations on E- safety provided to parents at regular points in the school E- safety calendar.
It is assumed that pupils and staff will not be granted access to school internet and related internet technologies until the AUP agreement has been signed.

**How does the school self- evaluate E-safety and AUP provision?**
• E-safety permeates all aspects of school internet, intranet and technology usage within school and the wider school community.
• E-safety is referenced in and relates to the following school policies and development / improvement planning:
• For example: SEF, school development plan, data protection policy, photo permissions policy, PSHE policy, SRE policy, behaviour policy, rewards and sanctions policy, child protection policy, safeguarding policy, ICT policy, complaints policy, safer working practices policy and Prevent Policy.

**Useful links to external organisations:**
**Ofsted:**
• http://www.ofsted.gov.uk/resources/handbook-for-inspection-of-schools-september-2012
•http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-andacademies-september-2
• http://www.ofsted.gov.uk/news/staying-safe-online
• http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies
• http://www.ofsted.gov.uk/resources/ict-schools-2008-11

**DfE:**
• https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

**CEOP:**
• http://www.ceop.police.uk/safety-centre/
• http://childnet-int.org/

**UK Safer Internet Centre:**
• http://www.saferinternet.org.uk/safer-internet-day
• http://www.saferinternet.org.uk/

**Internet Watch Foundation:**
• www.iwf.org.uk
• https://www.iwf.org.uk/members/get-involved
• https://www.iwf.org.uk/resources

**Links to training:**
E-safety Support: online refresher training https://www.e-safetysupport.com/resources/details/?resource_type=online_training
CEOP: http://www.ceop.police.uk/training/
NAACE: free e-safety online training: http://www.naace.co.uk/ictcpd4free
EPICT: offline and online e-safety training: http://www.epict.co.uk/#!esafety

**Movies and presentations:**
http://www.swgfl.org.uk/Staying-Safe/e-safety-Movies
**Other publications:**

- Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/byronreview/
- Ofcom’s response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecomsresearch/byron/