ESTABLISHED 1906

Lord's School

E-Safety Policy

Oct 2019 - Oct 2020

Table of Contents

1 Introduction

National guidance suggests that it is essential for schools to take a leading role in e-safety. in its "Safeguarding Children in a Digital World" Becta*, suggested:

"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, it recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of IT, too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

The development and expansion of the use of IT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level IT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that IT can bring to teaching and learning. Schools have made a significant investment, both financially and physically, to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.
The policy will also form part of the school's protection from legal challenge relating to the use of IT.

*Becta - British Educational Communications and Technology Agency

2 Background and Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students / pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

3 Development, Monitoring and Review

This e-safety policy has been developed by a group that included the following:

Head Teacher Responsible for Safeguarding
• Teachers
• Students

3.1 Schedule for Development, Monitoring and Review

The E-Safety Policy will be reviewed 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.

The next anticipated review date will be: April 2017

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

POLICE

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

4 Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such 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. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. Where necessary and appropriate the community police will be informed.

5 Teaching and Learning

5.1 The Importance of Internet Use

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through IT and Internet use.

- ✓ Internet use is part of the statutory curriculum and is a necessary tool for learning.

- ✓ The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- ✓ Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- ✓ The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance•the•school's•management•functions.

5.2 Benefits of Internet Use in Education

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries
- Inclusion in the National Education Network which connects all UK schools
- Educational and cultural exchanges between pupils worldwide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments
- Educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Access to learning wherever and whenever convenient.

5.3 Use of the Internet to Enhance Learning

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material is taught.

- ✓ The•school's•Internet•access is designed to enhance and extend education.
- ✓ Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- ✓ The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law. Plagiarism is an offence and will be strictly dealt with.

5.4 Pupil Evaluation of Internet and Online Content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as animal testing, nuclear energy etc. provide an opportunity for pupils to develop skills in evaluating Internet content.

- ✓ Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.
- ✓ Pupils use age-appropriate tools to research Internet content.

6 Managing Information Systems

6.1 Information Systems Security and Maintenance

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

IT security is a complex issue which cannot be dealt with adequately within this document.

Local Area Network (LAN) security issues include:

- Users must act reasonably - e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations are secured against user mistakes and deliberate actions.
- Servers are located securely and physical access is restricted.
- Virus protection for the whole network is installed and is current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA encryption.

- ✓ The security of the school information systems and users is reviewed regularly.
- ✓ Virus protection is updated regularly.
- ✓ Unapproved software will not be allowed.
- ✓ Files held•on•the•school's•network•are regularly checked.
- ✓ The IT Operations Manager reviews system capacity regularly.
- ✓ The use of user logins and passwords to access the school network is enforced.

6.2 Email Management

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between neighbouring schools and in different countries can be created.

The implications of email use for the school and pupils needs to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- ✓ Pupils may only use approved email accounts for school purposes.
- ✓ Pupils must immediately tell a designated member of staff if they receive offensive email.
- ✓ Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- ✓ Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- ✓ Access in school to external personal email accounts may be blocked.
- ✓ Excessive social email use can interfere with learning and will be restricted.
- ✓ The forwarding of chain messages is not permitted.
- ✓ Staff should not use personal email accounts during school hours or for professional purposes.

6.3 Management of Published Content

Many schools have created excellent websites and communication channels, which inspire pupils to publish work of a high standard. Websites can celebrate pupils' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Sensitive information about schools and pupils could be found in a newsletter but a school's website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint.

- ✓ The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

- ✓ Email addresses will be published carefully online, to avoid being harvested for spam

- ✓ The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

- ✓ The school website complies with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

6.4 Publication of Pupils Work or Images

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity.

Images of a pupil should not be published without the parent's or carer's written permission.

- ✓ Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- ✓ Pupils' full names will not be used anywhere on the website, particularly in association with photographs without parents/carers permission.
- ✓ Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- ✓ Written consent will be kept by the school where pupils' images are used for publicity purposes until the image is no longer in use.

6.5 Management of Social Networking and Social Media

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- ✓ The school will control access to social media and social networking sites.

- ✓ Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- ✓ Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- ✓ All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- ✓ Concerns•regarding•students'•use•of•social•networking,•social•media•and personal publishing sites (in or out of school) will be raised with their parents/carers,•particularly•when•concerning•students'•underage•use•of•sites.

- ✓ Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour is outlined in the school Acceptable Use Policy.

6.6 Internet Filtering

It is important to recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.

Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- ✓ The school has a clear procedure for reporting breaches of filtering. Which should be reported immediately to Mrs Ainsworth or Mr Ainsworth. All members of the school community (all staff and all pupils) will be aware of this procedure.
- ✓ If staff or pupils discover unsuitable sites, the URL will be reported to the Mr Ainsworth who will then record the incident and escalate the concern as appropriate.
- ✓ The School filtering system will block all sites considered unsuitable.
- ✓ The School will ensure that regular checks are made to ensure that the filtering methods selected are effective.

6.7 Management of Videoconferencing

Videoconferencing is not available within Lord's School

6.8 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as•a•pupil•using•a•phone•to•video•a•teacher's•reaction•in•a•difficult•situation.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils and families.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive•messages•should•be•dealt•with•under•the•school's•behaviour•and/or•anti-bullying policies.

- ✓ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- ✓ Pupils will be instructed about safe and appropriate use of personal devices both on and off site.

6.9 Protection of Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The•Data•Protection•Act•1998•(“the•Act”)•gives•individuals•the•right•to•know•what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed•in•line•with•individual’s•rights
- Kept secure
- Transferred only to other countries with suitable security measures

- ✓ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

7 Policy Decisions

7.1 Internet Access Authorisation

The school is aware that students should not be prevented from accessing the internet unless the parents have specifically denied permission or the child is subject to a sanction as part of the school behaviour policy.

- ✓ Parents will be informed that pupils will be provided with supervised Internet access.

- ✓ When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

7.2 Assessment of Risks

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

Risks can be considerably greater where tools are used which are beyond the schools control such as most popular social media sites.

- ✓ The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

- ✓ The school will audit IT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

- ✓ The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.

- ✓ Methods to identify, assess and minimise risks will be reviewed regularly.

7.3 School Response to Incidents of Concern

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used.

E-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff should also help develop•a•safe•culture•by•observing•each•other's•behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Senior Leader.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school will determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

- ✓ All members of the school community will be informed about the procedure for reporting e-Safety concerns
- ✓ The Designated Senior Leader (Mr Ainsworth) will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- ✓ The school will manage e-Safety incidents in accordance with the school behaviour policy where appropriate.
- ✓ The school will inform parents/carers of any incidents of concern as and when required.
- ✓ After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- ✓ Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the e-Safety officer and escalate the concern to the Police.

7.4 E-Safety Complaints

Parents, teachers•and•pupils•should•know•how•to•use•the•school's•complaints procedure.

The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. e-Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required,•which•should•be•linked•to•the•school's•disciplinary•policy.•Potential•child protection or illegal issues must be referred to the school Designated Senior Leader.

- ✓ Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- ✓ Any complaint about staff misuse will be referred to the Headteacher.
- ✓ All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- ✓ Pupils and parents will be informed of the complaints procedure.
- ✓ Parents and pupils will need to work in partnership with the school to resolve issues.
- ✓ All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- ✓ Any•issues•(including•sanctions)•will•be•dealt•with•according•to•the•school's disciplinary, behaviour and child protection procedures.
- ✓ All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

7.5 Community Internet Use

Regarding internet access in the community, there is a fine balance between ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community.

- ✓ The school will liaise, where possible, with local organisations to establish a common approach to e–Safety.
- ✓ The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- ✓ The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

7.6 Cyber Bullying

Cyberbullying•can•be•defined•as•“The•use•of•Information•Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” - DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects.

A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school’s•behaviour•policy•which•must be communicated to all pupils, school staff and parents

- Gives Headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feel that an offence may have been committed they should seek assistance from the police.

- ✓ Cyberbullying (along with all other forms of bullying) of any member of the school•community•will•not•be•tolerated.•Full•details•are•set•out•in•the•school’s policy on anti-bullying and behaviour.

- ✓ There are clear procedures in place to support anyone in the school community affected by cyberbullying.

- ✓ All incidents of cyberbullying reported to the school will be recorded.

- ✓ There are clear procedures in place to investigate incidents or allegations of Cyberbullying.

- ✓ Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- ✓ The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- ✓ Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

- ✓ Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive
    - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time.
    - Other school sanctions for pupils and staff may also be used in accordance to the schools Anti-Bullying, Behaviour Policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

7.6.1 "Revenge Pornography"

Sharing private material as "revenge porn" online is illegal in England and Wales. The legislation, which went through Parliament as an amendment to the Criminal Justice and Courts Bill, came into force on Monday April 13th 2015.

Clause 33 in the legislation classes "revenge porn" as:

Disclosing private sexual photographs and films with intent to cause distress

1. It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made-

a) without the consent of an individual who appears in the photograph or film, and
b) with the intention of causing that individual distress.

2. But it is not an offence under this section for the person to disclose the photograph or film to the individual mentioned in subsection (1)(a) and (b).

7.7 Use of the Virtual Learning Environment

An effective learning platform or virtual learning environment (VLE) offers the school a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- ✓ Pupils/staff will be advised about acceptable conduct and use when using the VLE

- ✓ Only members of the current pupil, parent/carers and staff community will have access to the VLE.

- ✓ All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.

- ✓ When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled.

7.8 Use of Mobile Phones and Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players•etc.•are•considered•to•be•an•everyday•item•in•today's•society•and•even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texts, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their use can render pupils or staff subject to cyberbullying.
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

A policy which prohibits pupils from taking mobile phones to school could be considered to be unreasonable and unrealistic for schools to achieve. Many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a phone and many staff also use mobile phones to stay in touch with family.

Due to the widespread use of personal devices it is essential that the school takes steps to ensure mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms.

- ✓ The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.
- ✓ The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

- ✓ School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by Mr Ainsworth with the consent of the pupil or parent/carer.

- ✓ If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- ✓ Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

7.8.1 Pupils Use of Personal Devices

- ✓ If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

- ✓ Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate•examining•body.•This•may•result•in•the•student's•withdrawal•from either that examination or all examinations.

- ✓ If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- ✓ Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

7.8.2 Staff Use of Personal Devices

- ✓ Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

- ✓ Mobile Phones and•devices•will•be•switched•off•or•switched•to•'silent'•mode and Bluetooth•communication•should•be•"hidden"•or•switched•off.

- ✓ Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- ✓ If a member of staff breaches the school policy then disciplinary action may be taken.

8 Radicalisation and Extremism

The school's safeguarding policy which is available on our website (www.lordsschool.co.uk) and in school, covers Radicalisation and Extremism.

8.1 Indicators of Vulnerability to Extremism and Radicalisation

1. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

2. Extremism is defined by the Government in the Prevent Strategy as:
   Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

3. Extremism is defined by the Crown Prosecution Service as:
   The demonstration of unacceptable behaviour by using any means or medium to express views which:

   - Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
   - Seek to provoke others to terrorist acts.
   - Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
   - Foster hatred which might lead to inter-community violence in the UK.

4. There is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

5. Pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

6. Indicators of vulnerability include:

- Identity Crisis – the student / pupil is distanced from their cultural / religious heritage and experiences discomfort about their place in society.
- Personal Crisis – the student / pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.
- Personal Circumstances – migration; local community tensions; and events•affecting•the•student•/•pupil's•country•or•region•of•origin•may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.
- Unmet Aspirations – the student / pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.
- Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement / reintegration.
- Special Educational Need – students / pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.

7. However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.

8. More critical risk factors could include:

- Being in contact with extremist recruiters.
- Accessing violent extremist websites, especially those with a social networking element.
- Possessing or accessing violent extremist literature.
- Using extremist narratives and a global ideology to explain personal disadvantage.
- Justifying the use of violence to solve societal issues.
- Joining or seeking to join extremist organisations.
- Significant changes to appearance and / or behaviour.
- Experiencing a high level of social isolation resulting in issues of identity crisis and / or personal crisis.

8.2 Preventing Violent Extremism

- Ensuring that staff of the school are aware how to protecting students/pupils from radicalisation and involvement in terrorism.

- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.

- Raising awareness about the role and responsibilities in school in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Monitoring the effect in practice of the school's curriculum to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.

- Mrs Ainsworth acts as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.

- and is responsible for collating relevant information from in relation to referrals of vulnerable students / pupils into the Channel* process..

- Sharing any relevant additional information in a timely manner.

* Channel is a multi-agency approach to provide support to individuals who are at risk of being drawn into terrorist related activity. It is led by the West Midlands Police Counter-Terrorism Unit, and it aims to
  - Establish an effective multi-agency referral and intervention process to identify vulnerable individuals;
  - Safeguard individuals who might be vulnerable to being radicalised, so that they are not at risk of being drawn into terrorist-related activity; and
  - Provide early intervention to protect and divert people away from the risks they face and reduce vulnerability.

9 Policy Communication

9.1 Policy Introduction to Students

Many pupils are very familiar with culture of mobile and Internet use however as pupils' perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

- ✓ All users will be informed that network and Internet use will be monitored.
- ✓ An e–Safety training programme is established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- ✓ Safe and responsible use of the Internet and technology is reinforced across the curriculum and subject areas.
- ✓ Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

9.2 Policy Introduction to Staff

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies.

All staff must understand that the rules for information systems misuse for school employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their IT or internet use either on or off site, they should discuss this with their manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

IT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the school e–Safety Policy.

- ✓ The e–Safety Policy will be formally provided to and discussed with all members of staff.
- ✓ Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- ✓ Staff who manage filtering systems or monitor IT use will be supervised by the Senior Management and have clear procedures for reporting issues.
- ✓ All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

9.3 Parental Support

Internet use in•pupils'•homes•is•increasing•rapidly,•encouraged•by•low•cost•access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to•check•whether•their•child's•use•elsewhere•in•the•community•is•covered•by•an appropriate use policy.

- ✓ Parents'•attention will be drawn to the school e–Safety on the school website.
- ✓ A partnership approach to e-Safety at home and at school with parents will be Encouraged.
- ✓ Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- ✓ Interested•parents•will•be•referred•to•organisations•listed•in•the•"e–Safety Contacts•and•References•section".

10 E-Safety Contacts and References

360 Safe Self Review Tool: http://www.360safe.org.uk/

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

11 Legal Framework

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victims' sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc… fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools should have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

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.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

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 someone else's password to access files)
• Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud)
• Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

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

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

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

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

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

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.

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.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

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.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

• Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.

• School staff are able to confiscate items such as mobile phones etc… when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.