OLDFIELD SCHOOL

ONLINE SAFETY POLICY

Last Review:	Nov 2017
Committee:	SLT
Date Ratified:	22/11/17
Next Review:	Nov 2019

Introduction

The growth of the internet and the development of mobile technology has created an exciting and stimulating world with great opportunities for students to explore, interact, learn and enjoy social interaction online.

However, the importance of treating online safety as an ever-present serious safeguarding issue is recognised. It is important to protect and educate both students and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community both in and outside of school.

The safeguarding aspects of online safety are evident in all our ICT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review. As with all other risks it is impossible to eliminate those risks completely. It is therefore essential to support all stakeholders in acquiring the skills to remain safe whilst accessing this technology.

This policy should be read in conjunction with the following policies -

- Information and Communication Technologies and Acceptable Use
- Safeguarding and Child Protection
- Anti-bullying
- Positive Behaviour for Learning
- Code of Conduct for staff
- Whistleblowing
- Mobile Phone and Electronic Devises
- Privacy
- Data Protection

- Other procedures to reflect how the school deals with online safety issues on a daily basis.

The documents referred to in this online safety policy have been developed by various groups including:

- Governors.
- Headteacher/Senior Leadership Team (SLT)/Designated Safeguarding Lead (DSL).
- ICT teaching and technical support staff.
- Teachers and support staff.
- Parents/carers.
- Students.

Objectives and Targets
This policy is aimed at making the use of electronic communication at Oldfield School as safe as possible. It applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

This policy aims to support the school community in understanding their responsibilities in ensuring safety when using technologies, including 3G & 4G whilst fully exploiting the power of these technologies to enhance educational outcomes.

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

The following sections outline:

- The roles and responsibilities for online safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles (Appendix 1)
- How the infrastructure is managed (Appendix 2)
- How online safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.
- Awareness of and dealing with inappropriate use of electronic media (Appendix 3 & 4)
- Advice and support for all stakeholders (Appendix 5)

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

- A planned online safety programme is provided as part of ICT/PSHE/other lessons – this includes both the use of ICT and new technologies in school and outside school.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities. This includes participation in the annual national campaign of Safer Internet Day.

- Students are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Students are helped to understand the need for the student acceptable computer usage agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students are taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet are posted in all relevant rooms and/or displayed on log-on screens.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages in the use of ICT across the curriculum.

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

Using Digital and Video Images

- When using digital images, staff inform and educate students about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images. Permission from parents or carers will be obtained and stored on SIMS.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers

comment on any activities involving other students in the digital / video images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff will ensure that they comply with the secure data handling policy by:

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

The school will ensure that -

- Only the minimum amount of personal data is held. This amount is not held for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". That the school follows our Data Protection policy.
- Risk assessments are carried out
- There are clear arrangements for the security, storage and transfer of personal data as well as the routines for the deletion and disposal of data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Communications

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

- All students read, accept and adhere to the Acceptable Use Policy which is shown every time they log on.
- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.

- Users are expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)
- Users must immediately report, to the Designated Safeguarding Lead (DSL), in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.
- Any digital communication between staff and students or parents/carers must be professional in tone and content. A copy of any such communication should be kept. Personal addresses, mobiles etc. must not be used for these communications.
- Personal information should not be posted on the school website and only official school email addresses should be used to identify members of staff.
- A breach of any of this guidance may result in disciplinary action.

Unsuitable/Inappropriate Activities

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

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

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

Training

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

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

The Assistant Headteacher (Inclusion) will receive training at regular intervals (at least bi-annually) and by reviewing national / local guidance documents.

The DSL and/or IT technicians provide additional support/advice/guidance/ training to individuals and whole staff body when required.

Governors should take part in online safety training/awareness sessions, with particular importance to members of the governing body responsible for safeguarding / ICT / Health and Safety.

Parents /carers should be provided with information about the school's online and acceptable use policies and how to help keep young people safe when using ICT at home. An information evening will be held annually to provide support/advice for parents.

Monitoring and reviewing

This policy will be reviewed annually by the Governing Body. Consultation with the whole school community has taken place through a range of formal and informal meetings.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity.
- Internal monitoring data for network activity.
- Surveys/questionnaires of students, parents/carers and staff.

The policy will be reviewed in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to online safety.

Appendix 1 - Roles and Responsibilities

Roles and Responsibilities - Governing Body

- Will discuss, review and endorse agreed strategies via the Personnel Committee and the Safeguarding Report on the workings of this policy.

Roles and Responsibilities – Headteacher and SLT

- The headteacher is responsible for ensuring the online safety of members of the school community.
- The deputy headteacher and Assistant Headteacher (Inclusion) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including the headteacher.
- The Education and Inspections Act 2006 empowers the headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-

bullying, or other e-safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

Roles and Responsibilities – Designated Safeguarding Lead (DSL)
The DSL is trained in online safety issues and will be aware of the potential for serious child protection issues to arise from:

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

The DSL -

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy and other related policies.
- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the local authority (LA).
- Liaises with school ICT technical staff.
- Liaises with the School Council and Staff Health and Safety committee. These bodies include online safety on their agendas and feedback their findings to the DSL.
- Reports regularly to the SLT and the Governing Body.

Roles and Responsibilities – ICT Technicians
The ICT Technicians:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/e-safety policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported for investigation.

- That monitoring software / systems are regularly updated.

Roles and Responsibilities – Teaching and Support Staff
Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy.

- They have read and understood the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies e.g. code of conduct policy.
- They report any suspected misuse or problem to the relevant member of staff for investigation/action/sanction.
- Digital communications with students, e.g. email should be on a professional level and only carried out using official school systems.
- Students understand and follow the school online safety policy and the student acceptable computer usage policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the online safety issues pertaining to email and social media usage.
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Roles and Responsibilities – Students

Students:

- Are responsible for using the school ICT systems in accordance with the student acceptable computer usage policy and agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.
- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school.

Roles and Responsibilities – Parents/Carers

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

- Parents and carers are responsible for endorsing the student acceptable computer usage agreement.

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

- Parents' evenings.
- Newsletters/Magazines.
- Letters.
- Website.
- Information about all relevant national/local e-safety campaigns/literature.

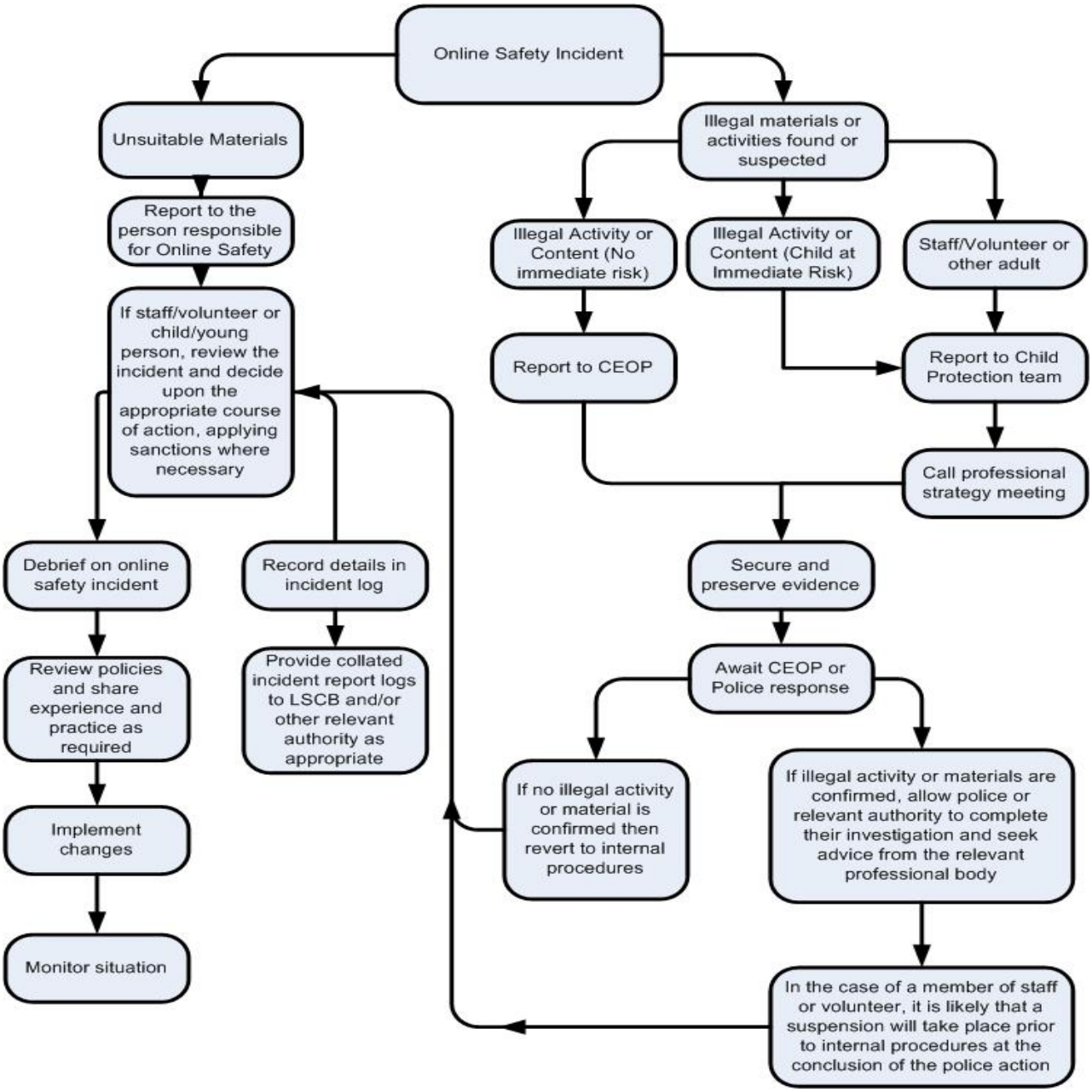
- Information about useful organisations /support services for reporting online safety issues (see appendix 2).

APPENDIX 2 Management of Infrastructure

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

- School ICT systems are managed in ways that ensure that the school meets the online safety technical requirements outlined in the acceptable computer usage policy and any relevant LA online safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the ICT Technicians and are reviewed regularly.
- All users are provided with a username and password by the ICT Technicians.
- The 'master/administrator' passwords for the school ICT system, used by the ICT Technicians are also available to the Headteacher or Deputy Headteacher and kept in a secure place (school safe).
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the South West Grid for Learning.
- Any filtering issues should be reported immediately to the ICT Technicians.
- School ICT Technicians regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.
- Appropriate security measures are in place to protect the servers, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.
- An agreement is signed by members of staff in possession of school provided laptops regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up-to-date anti-virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Appendix 3 - Responding to an online safety incident



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 4 - Using the Internet Safely

Annually students are reminded of the Acceptable Use Policy. This document is explained through the tutorial programme, subject teachers, and assemblies. Every time a student logs on in school or remotely a copy of this is displayed and agreed.

Students are taught to recognise the potential risks online including -

- Access to illegal, harmful or inappropriate images or other content

- Unauthorised access to / loss of/ sharing of personal information including identity fraud.

- The risk of being subject to grooming by those with whom they make contact on the internet including the risks of CSE / Radicalisation.

- The sharing and distribution of personal images without an individual's consent or knowledge e.g. sexting/sending nudes.

- Cyberbullying.

- Access to unsuitable video, internet games or the illegal downloading of music/video files.

- The impact on a student's mental/physical wellbeing.

- Inappropriate communication / contact with others including strangers.

Managing incidents:

- Students should report any concern or worry they have, regarding online safety to either their tutor, Head of Year, subject teacher or member of the Pastoral team or via the SWGFL Whisper / CEOP button on the school website.

- Staff should inform their line manager of any worries/concerns. If appropriate, the school's disciplinary procedures will be followed.

- The Designated Safeguarding Lead (DSL) should be informed if anyone's safety or wellbeing is considered to be at risk. It may be necessary for the DSL to inform outside agencies e.g. the police/social care/ Local Designated Safeguarding Officer.

Cyberbullying

As students spend an increasing amount of time online the potential risk has increased. As a school we have a responsibility to regulate the behaviour of students both in and outside of school and will impose disciplinary sanctions for inappropriate behaviour. This includes incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of school but is 'brought into' school. However, parents are always advised to contact the police and the service provided if incident of cyber-bullying take place.

Cyberbullying is when one person or a group of people aim to threaten, tease or embarrass someone else by using a mobile phone, the internet or other technologies. Cyber bullying can take place through -

- Sending abusive instant messenger and chatroom messages about a person directly to them or to other people.

- Sending email that can be threatening or upsetting

- Using social networking sites (e.g. Snapchat) to set up false profiles to humiliate and abuse.

- Sending humiliating or abusive text or video messages, as well as photo messages and phone calls.

- Sharing photos and / or videos of a person without their informed consent and using those images to humiliate or abuse that person.

Dealing with Cyber Bullying - Advice for parents

- Report abuse to the providers of the service concerned.

- Print out and/or keep any abusive messages or images.

- Involve the police if it is persistent and inform school. The school's anti-bullying policy will then be followed.

- Parents can use the report an incident links on the school website to report an incident to CEOP.

- If bullying takes place outside of school, then it is the parents' responsibility to act in the first instance and if necessary inform the appropriate agencies.

- School will offer support and advice and take any reasonable action to ensure such incidents are not repeated and that it does not affect the education of all involved.

Appendix 5 - Useful organisations/support services for reporting online safety issues

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

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

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

Media Content Inappropriate for Children
If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through *ParentPort* at www.parentport.org.uk. Click on 'Make a Complaint' and ParentPort will take you straight to the right place to complain to.

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

Getting Help/Advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.
- Cybermentors: For bullying issues, go on-line and talk to other children to get help and support www.cybermentors.org.uk. Cybermentors is run by Beatbullying.
- Youth 2 Youth: A young persons' helpline which offers confidential peer support via telephone, email and online chat – www.youth2youth.co.uk.
- Get Connected: A free confidential helpline for young people, open 1pm-11pm every day. Tel 0808 8084994.

Getting Help/Advice: for parents

- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk

- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 8pm, on 08451 205204 www.kidscape.org.uk.

Getting Help/Advice: for professionals working with children

- *Professionals online safety helpline*: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with on-line safety issues. The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0844 3814772 (calls on this number are charged at local call rate).

Appendix 6 - Government Legislation

The school adheres to all government legislation regarding online safety. The following acts of parliament and guidance are followed.

- Acts of Parliament relevant to e-safety in schools
- Communications Act 2003 (section 127)
- Computer Misuse Act 1990 (sections 1–3)
- Copyright, Design and Patents Act 1988
- Criminal Justice Act 2003
- Criminal Justice and Immigration Act 2008 (section 63)
- Data Protection Act 1998
- Education and Inspections Act 2006
- Malicious Communications Act 1988 (section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- Public Order Act 1986 (sections 17–29)
- Racial and Religious Hatred Act 2006
- Regulation of Investigatory Powers Act 2000
- Sexual Offences Act 2003