Online Safety Policy

Date policy last reviewed: _____

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

The use of information and communication technologies (ICT) including the Internet has developed over the past 25 years and now involves every pupil and member of staff. Online-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. Pupils interact with new technologies on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger. Online-safety highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences. Schools have a duty to decide on the right balance between controlling access, setting rules and educating students for responsible use.

1.1 WRITING AND REVIEWING THE ONLINE-SAFETY POLICY

- The Online-Safety Policy is part of the school policy review cycle and relates to other policies including those for Computing, Health and Safety, Anti- Bullying and for Safeguarding and Child Protection;
- The school will appoint an online-Safety Coordinator. This may be the Designated Safeguarding Lead as the roles overlap. It is not a technical role;
- Our Online-Safety Policy has been written by the school, building on government guidance. It has been agreed by the senior leadership team and approved by staff and governors;
- The Online-Safety Policy and its implementation will be reviewed annually.

1.2 TEACHING AND LEARNING

1.2.1 Why the Internet and digital communications are important

- 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;
- Internet use is part of the statutory curriculum and a necessary tool for learning;
- The Internet is an essential element in 21st century 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 will need to learn how to evaluate Internet information and to take care of their own safety and security.

1.2.2 How the Internet benefits education

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils world-wide;
- 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 support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with West Sussex County Council and DfE;
- Access to learning wherever and whenever convenient.

1.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils;
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils;
- Staff will guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity;
- Staff will teach search skills and educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law;
- Pupils should be made aware that not all of the materials that they read will be accurate just because they are published on the internet.

1.3 MANAGING INTERNET ACCESS

1.3.1 Information system security

- School IT systems security will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with the Local Authority and technical support.

1.3.2 Email

- Pupils will only have access to email through a whole-class or group e-mail address, which will be used under the supervision of the class teacher and network manager;
- Access in school to external personal email accounts by staff may be blocked;
- Emails by staff, written to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- The forwarding of chain letters is not permitted.

1.3.3 Published content and the school web site

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

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupil images cannot be misused;
- Pupils full names will not be used anywhere on a school website or other online space, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website;
- Written permission from parents or carers will be obtained before work can be published. This is included in the Online-safety Acceptable Use Agreement (Appendix 7).

1.3.5 Social networking and personal publishing

- The school will block access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- 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, specific interests and clubs etc...

1.3.6 Managing filtering

- The school will work with WSCC, Entrust and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved;
- If staff or pupils discover unsuitable sites, the URL must be reported to the Online-Safety Coordinator.

1.3.7 Managing videoconferencing & webcam use

- Staff and pupils do not currently have access to videoconferencing or a web cam.

1.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications;
- Pupils are not permitted to bring mobile phones into school;
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location;
- Appropriate use of the Learning Platform is outlined in the Acceptable Use Policy for Virtual Learning Environments**.**

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations, 2018.

1.4 POLICY DECISIONS

1.4.1 Authorising Internet access

- **All staff must read and sign the Staff Code of Conduct for IT before using any school IT resources.** *Please see Appendix 6;*
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems;
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials;
- Any person not directly employed by the school will be asked to sign an, acceptable use of school IT resources before being allowed to access the internet from the school site.

1.4.2 Assessing risks

- 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. Neither the school nor WSCC can accept liability for the material accessed, or any consequences resulting from Internet use;

- The school will audit IT use to establish if the online-safety policy is adequate and that the implementation of the online-safety policy is appropriate. (Appendix 4)

1.4.3 Handling online-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff;
- Any complaint about staff misuse must be referred to the headteacher;
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Refer to the BECTA flowchart for responding to internet safety incidents in school, Appendix 5);
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

1.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to online-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.

1.5 COMMUNICATIONS POLICY

1.5.1 Introducing the Online-Safety Policy to pupils

- Online-safety will be incorporated into Computing cross curricular planning at an appropriate level for each year group;
- Pupils will be involved in devising a class promise or charter for safe internet use, which will be displayed in rooms with Internet access.

1.5.2 Staff and the Online-Safety policy

- All staff will be given the School Online-Safety Policy and its application and importance explained;
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues;
- Staff training in safe and responsible Internet use and on the school Online-Safety Policy will be provided as required.

1.5.3 Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School Online-Safety Policy on the school website, virtual learning environment and in newsletters;
- Interested parents will be referred to organisations listed in Appendix 3;
- Internet issues will be handled sensitively, and parents will be advised accordingly;
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

2.0 LEGAL FRAMEWORK

Notes on the legal framework
This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice. Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

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

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff 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 already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. More information about the 2003 Act can be found at www.gmc-uk.org/**sex**_offences_act_2.pdf_48793788.pdf.

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.

General Data Protection Regulations 2018
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 regulation 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); or

- 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 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.

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

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

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

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.

APPENDIX 1: INTERNET USE - POSSIBLE TEACHING AND LEARNING ACTIVITIES

Activities - Key online-safety issues

- **Relevant Websites.** Creating web directories to provide easy access to suitable websites. Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials. Web directories e.g. bookmarks and favourites.
- **Using search engines to access information from a range of websites.** Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. Web quests e.g. Ask Jeeves for kids, Yahooligans, CBBC Search, Kidsclick.
- **Exchanging information with other pupils.** Pupils need to comply with the AUP which will be reinforced by staff and parents. Information exchanged needs to be relevant to the topic. Class teachers will monitor use.
- **Publishing pupils' work on school and other websites.** Pupil and parental consent should be sought prior to publication. Pupil's full names and other personal information should be omitted. Pupils' work should only be published on moderated sites and by the school administrator.
- **Publishing images including photographs of pupils.** Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.
- **Audio and video conferencing to gather information and share pupils work.** Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers. Pupils should be supervised.

APPENDIX 2: USEFUL RESOURCES FOR TEACHERS

BBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing/
Becta http://schools.becta.org.uk/index.php?section=is
Chat Danger www.chatdanger.com/
Child Exploitation and Online Protection Centre www.ceop.gov.uk/
Childnet www.childnet-int.org/
Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Kidsmart www.kidsmart.org.uk/
Think U Know www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

APPENDIX 3: USEFUL RESOURCES FOR PARENTS

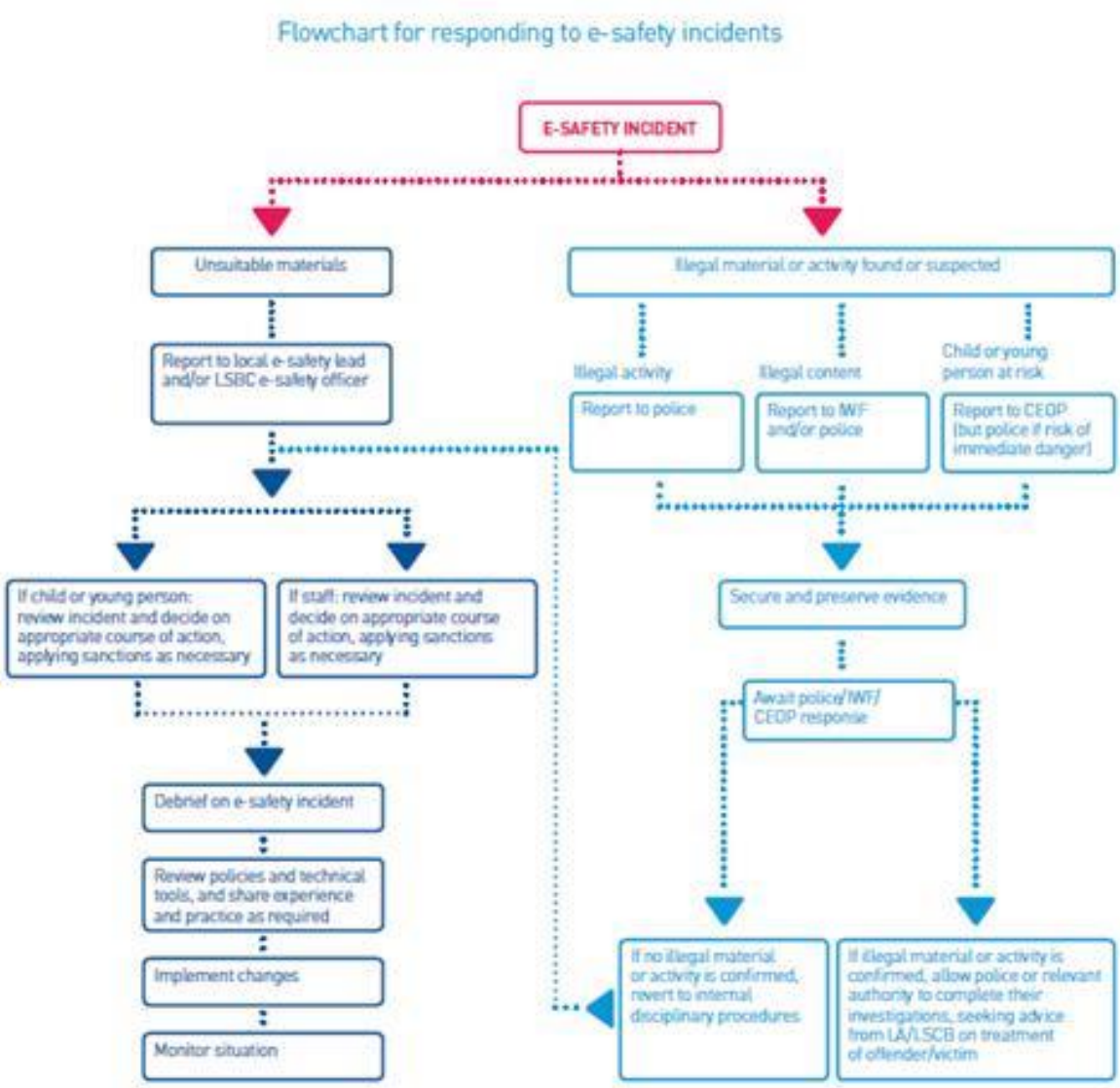
Care for the family www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD http://publications.teachernet.gov.uk
Family Online Safe Institute www.fosi.org Internet Watch Foundation www.iwf.org.uk
Parents Centre www.parentscentre.gov.uk
Internet Safety Zone www.internetsafetyzone.com

APPENDIX 4: SAFETY AUDIT – PRIMARY/SPECIAL

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for online-safety. Many staff could contribute to the audit including: Designated Safeguarding Lead, AHT for Inclusion, Online-Safety Coordinator, Network Manager and Headteacher.

1. Has the school got an online-Safety Policy that complies with WSCC guidance? Y/N
2. Date of latest update (at least annual):
3. The school e-safety policy was agreed by governors on:
4. The policy is available for staff at:
5. The policy is available for parents/carers at:
6. The responsible member of the Senior Leadership Team is:
7. The responsible member of the Governing Body is:
8. The Designated Safeguarding Lead is:
9. The Online-Safety Coordinator is:
10. Has online-safety training been provided for both pupils and staff? Y/N
11. Is there a clear procedure for a response to an incident of concern? Y/N
12. Have online-safety materials from CEOP and Becta been obtained? Y/N
13. Do all staff sign a Code of Conduct for IT on appointment? Y/N
14. Are all pupils aware of the School's online-safety rules? Y/N
15. Are online-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? Y/N
16. Do parents/carers sign and return an agreement that their child will comply with the school online-safety rules? Y/N
17. Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? Y/N
18. Has an IT security audit been initiated by SLT, possibly using external expertise? Y/N
19. Is personal data collected, stored and used according to the principles of the General Data Protection Regulations? Y/N
20. Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements? Y/N
21. Has the school-level filtering been designed to reflect educational objectives and approved by SLT? Y/N

APPENDIX 5: BECTA FLOWCHART FOR RESPONDING TO INTERNET SAFETY INCIDENTS IN SCHOOL.



APPENDIX 6

Maidenbower Infant School Staff Code of Conduct for IT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner;
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business;
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher;
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance;
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager;
- I will not install any software or hardware without permission;
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely;
- I will respect copyright and intellectual property rights;
- I will report any incidents of concern regarding children's safety to the Online-Safety Coordinator, the Designated Safeguarding Lead or Headteacher;
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted;
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. I have read, understood and accept the Staff Code of Conduct for IT.

Signed: …… Capitals: …… Date: ……

Accepted for school: …….. Capitals: ……

APPENDIX 7: ONLINE-SAFETY - ACCEPTABLE USE AGREEMENT

These online-safety rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use;
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and social networking, and that IT use may also include personal IT devices when used for school business;
- I understand that it is a criminal offence to use a computer or network for a purpose not permitted by the school;
- I understand that the irresponsible use of the network and internet will result in the loss of network or internet access, and the school may instigate additional sanctions. For serious breaches, the school may involve the police;
- I agree that network access must be made via the user's authorised account and password, which must not be given to any other person;
- I understand that users may not install or run software on the network;
- I understand that all network and internet use must be appropriate to education;
- I agree that all copyright and intellectual property rights must be respected;
- I understand that all messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers;
- I understand that anonymous messages and chain letters are not permitted;
- I understand that I must take care not to reveal personal information through email, personal publishing, blogs or messaging;
- I agree to use school managed blogs, wikis and discussion groups appropriately and politely;
- I understand that the school IT systems may not be used for private purposes, unless the Headteacher has given specific permission;
- I agree that any inappropriate access to materials on the network or internet will be reported to a teacher;
- I understand that I must be socially responsible with regard to using the internet and other communication technologies, including treating others with respect, and reporting instances of online bullying;

The school may exercise its right to monitor the use of the school's computer systems, (including access to websites, the interception of email and the deletion of inappropriate materials) where it believes unauthorised use of the school's computer system may be taking place, or that the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.