

# Brimsham Green School

# E-SAFETY POLICY

Version 6.0  
5.3.2010

# Contents

<b>INTRODUCTION</b> .....	<b>3</b>
<b>BACKGROUND / RATIONALE BACKGROUND / RATIONALE</b> .....	<b>4</b>
<b>DEVELOPMENT / MONITORING / REVIEW OF THIS POLICY</b> .....	<b>5</b>
<b>SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW</b> .....	<b>6</b>
<b>SCOPE OF THE POLICY</b> .....	<b>7</b>
<b>ROLES AND RESPONSIBILITIES</b> .....	<b>8</b>
GOVERNORS: .....	8
HEADTEACHER AND SENIOR LEADERS: .....	8
E-SAFETY OFFICER .....	8
HEAD OF ICT: .....	8
NETWORK MANAGER / ICT TECHNICAL STAFF: .....	9
TEACHING AND SUPPORT STAFF.....	9
CHILD PROTECTION OFFICER .....	9
STUDENTS: .....	9
PARENTS / CARERS .....	10
<b>POLICY STATEMENTS</b> .....	<b>11</b>
EDUCATION – STUDENTS .....	11
EDUCATION – PARENTS / CARERS .....	11
EDUCATION & TRAINING – STAFF .....	11
TRAINING – GOVERNORS.....	11
TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING.....	12
CURRICULUM .....	12
USE OF DIGITAL AND VIDEO IMAGES - PHOTOGRAPHIC, VIDEO.....	13
DATA PROTECTION.....	13
COMMUNICATIONS .....	13
RESPONDING TO INCIDENTS OF MISUSE.....	14
<b>APPENDIX 1 – CURRICULUM OUTLINE</b> .....	<b>17</b>
<b>APPENDIX 2 – STUDENT AND PARENT/CARER ACCEPTABLE USE POLICY</b> .....	<b>18</b>
<b>APPENDIX 3 - STAFF ACCEPTABLE USE POLICY AGREEMENT</b> .....	<b>21</b>
<b>APPENDIX 4 - SCHOOL FILTERING POLICY</b> .....	<b>23</b>
<b>APPENDIX 5 - SCHOOL PASSWORD SECURITY POLICY</b> .....	<b>24</b>
<b>APPENDIX 6 – ACTION FLOW CHARTS</b> .....	<b>26</b>
<b>APPENDIX 7 – RULES FOR RESPONSIBLE USE OF ICT</b> .....	<b>27</b>
<b>APPENDIX 8 - LEGISLATION</b> .....	<b>28</b>

## Introduction

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT 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 ICT can bring to teaching and learning. Brimsham Green School has 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.” Brimsham Green School through this e-safety policy, ensures that statutory obligations are met 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 ICT.

## Background / Rationale Background / 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 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 development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

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
- Unauthorized 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 (eg 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' / pupils' 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.

## Development / Monitoring / Review of this Policy

This draft e-safety policy has been developed following a review of existing policies and resources. The review took place in January 2010 and included

- Headteacher
- Deputy Head and Child Protection Officer
- Business Manager - SLT
- Head of ICT - Teacher
- Network Manager – ICT Technical staff

Previous consultation with the whole school community has taken place through the following:

- Staff meetings
- INSET Day
- Governors meeting / sub committee meeting
- School website / newsletters

It is intended that this new policy will be made public by:

- Staff meetings – May 18<sup>th</sup> 2010
- School / Student / Pupil Council
- INSET Day – each year at beginning of term 1, CPO/e-safety officer update
- Governors curriculum sub committee meeting, March 15<sup>th</sup> 2010.
- Parents evening
- School website / newsletters

## Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body	15 <sup>th</sup> March 2010
The implementation of this e-safety policy will be monitored by:	RC/AW
Monitoring will take place at regular intervals:	As item 1 on Agenda of each fortnightly meeting of ICT Technical group.
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:	Policy reviewed annually in July of each year.  Next review is July 2010.
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police liaison officer.

The school will monitor the impact of the policy using:

- Logs of reported incidents (maintained at k:\staff\e-safety)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students (eg Ofsted "Tell-us" survey)
  - parents / carers
  - staff

## Scope of the Policy

This policy 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.

The Education and Inspections Act 2006 empowers Headteachers, 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, 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.

## Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

### **Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors curriculum sub-committee receiving regular information about e-safety incidents and monitoring reports.

### **Headteacher and Senior Leaders:**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- The Headteacher is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer, through the dissemination of the meeting notes from the fortnightly ICT technical team meetings
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

### **E-Safety Officer**

- has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- reviews incident log with Head of ICT
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

### **Head of ICT:**

- takes day to day responsibility for ensuring that all students experience a coherent, thorough and planned curriculum experience that includes all aspects of e-safety.
- takes day to day responsibility for e-safety issues
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- provides advice and training for staff where appropriate
- ensures that ICT teaching staff are well prepared to deliver the ICT curriculum with reference to e-safety issues as appropriate
- monitors the delivery of e-safety curriculum to ensure it is effective and meets the needs of students
- this program should reflect changes in technology and will therefore need regular (at least annual) updating.
- liaises with the Network Manager to ensure that all measures are taken to maintain a secure ICT infrastructure

### **Network Manager / ICT Technical staff:**

The Network Manager is responsible for ensuring:

- 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 SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through an enforced password protection policy
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of all ICT systems are regularly monitored in order that any misuse / attempted misuse can be reported to the E-safety Officer

ICT technicians support the Network Manager in the configuration, operation and maintenance of the school systems to ensure they are not open to misuse.

### **Teaching and Support Staff**

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Head of ICT or other staff as shown in the grid 'responding to incidents of misuse – students'.
- digital communications with students (email / any future VLE / voice / website) should be on a professional level
- students understand and follow the school e-safety and acceptable use 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, extra curricular and extended school activities
- they are aware of e-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

### **Child Protection Officer**

should be trained in e-safety issues and 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

### **Students:**

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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. They should also know and understand school policies on the taking / use of images and on cyber-bullying

- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

### ***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. 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, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy
- accessing the school website and when available, VLE and on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

# Policy Statements

## **Education – students**

Whilst 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT / PHSE lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. See curriculum outline in appendix 1.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities. See outline in appendix 1.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems will be displayed in all ICT rooms and a clear link from the school Intranet home page
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## **Education – parents / carers**

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE when available
- Reference to the SWGfL Safe website
- Required signature of student acceptable use agreement in student planner

## **Education & Training – Staff**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- This E-Safety policy and its updates will be presented to and discussed by staff during INSET days
- The E-Safety Officer will provide advice / guidance / training as required to individuals as required

## **Training – Governors**

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

## **Technical – infrastructure / equipment, filtering and monitoring**

The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems – this will take place at fortnightly ICT technical team meetings
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password by the ICT technician in charge of user administration, under the guidance of the network manager, who will keep an up to date record of users and their usernames.
- The “administrator” passwords for the school ICT system, used by the Network Manager will be available to the Headteacher or other nominated senior leader and kept in the school safe
- Users will be made 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 SWGfL
- In addition the school has provided enhanced user-level filtering through the use of the “Smoothwall” filtering programme.
- The Network manager only will control the filtering system. In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Head of ICT. If the request is agreed, this action will be recorded.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager and E-safety Officer.
- Appropriate security measures are in place to protect the servers, firewalls, 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 for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system. The ICT Technician in charge of user administration will, under the guidance of the Network Manager, administer such access.
- Users will not be allowed to download executable files with the exception of ICT technical staff and the Head of ICT.
- Users will not be allowed to install software onto any school device, with the exception of ICT technical staff and the Head of ICT, all requests for such installation will be made through the Network Manager.
- The school infrastructure and individual workstations are protected by up to date virus software.

## **Curriculum**

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that 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.

- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

### ***Use of digital and video images - Photographic, Video***

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Students must not take, use, share, publish or distribute images of others without their permission
- 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.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

### ***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 must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. The school email system is fully encrypted.
- Store personal (to themselves or others) data only on school computers and devices that are secure and password protected. No such data should be stored on any removable media such as USB memory stick.

### ***Communications***

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

- 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 must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Use of mobile phones are subject to the same student and staff acceptable use policies and agreements as the use of any other communications device.

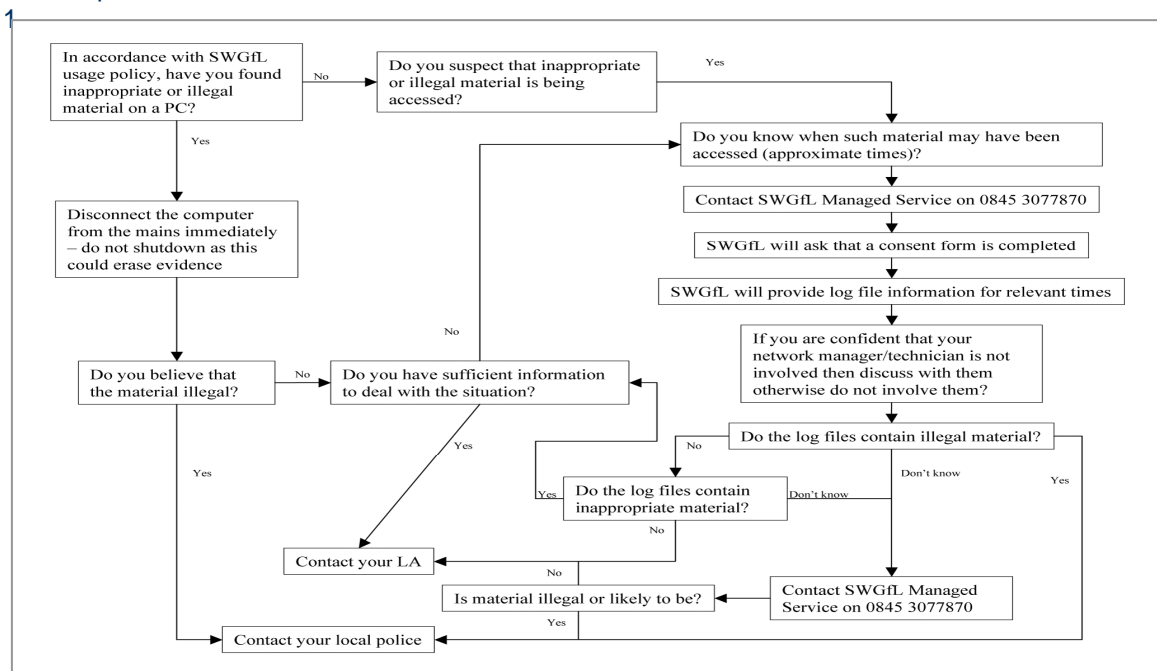
### **Responding to incidents of misuse**

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SWGfL flow chart – below and <http://www.swgfl.org.uk/safety/default.asp> should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed. This can be found on the SWGfL Safe website within the “Safety and Security booklet”. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate

manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

## Students

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year	Refer to E-safety/CPO	Refer to Headteacher	Refer to Police	Refer to Network  Manager / ICT Technicians	Refer to Head of ICT
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√
Unauthorised use of non-educational sites during lessons	√	√					
Unauthorised use of social networking / instant messaging / personal email	√	√					
Allowing others to access school network by sharing username and passwords	√					√	√
Attempting to access or accessing the school network, using another student's / pupil's account	√	√				√	√
Attempting to access or accessing the school network, using the account of a member of staff	√	√	√			√	√
Corrupting or destroying the data of other users	√	√				√	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√			√	√
Continued infringements of the above, following previous warnings or sanctions	√	√	√	√		√	√
Using proxy sites or other means to subvert the school's filtering system	√	√				√	√
Accidentally accessing offensive or pornographic material and failing to report the incident	√		√			√	√
Deliberately accessing or trying to access offensive or pornographic material	√	√	√			√	√

Sanctions, where appropriate, will follow school procedures.

## Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Network Manager	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		√	√	√	√	
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√					
Unauthorised downloading or uploading of files					√	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account					√	
Careless use of personal data eg holding or transferring data in an insecure manner	√	√				
Deliberate actions to breach data protection or network security rules	√	√				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		√			√	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		√			√	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√				
Using proxy sites or other means to subvert the school's filtering system		√			√	
Accidentally accessing offensive or pornographic material and failing to report the incident	√				√	
Deliberately accessing or trying to access offensive or pornographic material		√			√	
Continued infringements of the above, following previous warnings or sanctions		√			√	

Headteacher will decide on appropriate action.

# Appendix 1 – Curriculum Outline

## ICT Lessons

All students at Brimsham Green School have timetabled ICT lessons. Lesson 1 in September for every student will be an update on current e-safety issues and will include material related to cyber bullying. In addition to this ICT staff will highlight issues as they arise and relate to specific ICT activities undertaken during the course of teaching the ICT programme of study.

Unit 7.1, delivered in the autumn term includes activities to promote an understanding of the wide range in quality and accuracy of material found on the Internet. This work is developed in years 8 and 9 with units 8.1 and 9.1 taught in the Autumn term of each year to help students to become discerning users of the Internet with understanding of how to establish validity and potential bias of material. Issues of plagiarism and copyright infringement are integral to the GCSE syllabus content undertaken by all students in years 10 and 11.

## PSE/Citizenship lessons

One lesson in each year will have a particular focus of e-safety. These lessons will be planned by the Head of ICT in liaison with the Citizenship Officer. Outline:

Year 7 – Included in talk by community police officer

Year 8 – Included in 'Healthy Lifestyles' unit.

Year 9 – Included in 'Relationships and Sex Education' unit.

Year 10 – Included in 'Emotional and Mental Health' unit.

Year 11 – Included as part of Careers programme, 'Responsibility in Employment'.

## Assemblies

One assembly per year group per year will have a focus of e-safety. These assemblies will be planned by the head of ICT in liaison with Pastoral deputy and heads of year.

# Appendix 2 – Student and Parent/Carer Acceptable Use Policy

## School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

## Student Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password with care – I will not share it, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when on-line.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites under the direct instruction and supervision of a member of staff.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

## Student Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg PDAs, laptops, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student

Tutor

Signed (pupil)

Date

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

## Permission Form

Parent / Carers Name

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

## Appendix 3 - Staff Acceptable Use Policy Agreement

New technologies have become integral to the lives of adults, children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE, website etc) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

## Appendix 4 - School Filtering Policy

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the South West Grid for Learning (SWGfL) schools automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

### Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL / school filtering service must:

- be logged in change control logs
- be reported to a second responsible person (Head of ICT).

All users have a responsibility to report immediately to the Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Parents and students will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Staff users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the Network Manager should email [filtering@swgfl.org.uk](mailto:filtering@swgfl.org.uk) with the URL.

### Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the Head of ICT
- ICT Technical meetings
- Governors curriculum committee
- SWGfL / Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

## Appendix 5 - School Password Security Policy

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and any future Virtual Learning Environment (VLE).

### Responsibilities

The management of the password security policy will be the responsibility of the ICT Technician responsible for user accounts under the supervision of the Network Manager.

All users (adults and young people) will have responsibility 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.

Passwords for new users, and replacement passwords for existing users can be allocated by ICT Technician responsible for user accounts.

### Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in ICT and e-safety lessons (as detailed in Appendix 1)
- through the Acceptable Use Agreement

### Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the ICT Technical group.

All users will be provided with a username and password by ICT Technician responsible for user accounts who will keep an up to date record of users and their usernames

The following rules apply to the use of passwords:

- the password should be a minimum of 8 characters long and
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user

The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in the school safe.

## **Audit / Monitoring / Reporting / Review**

The Network manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

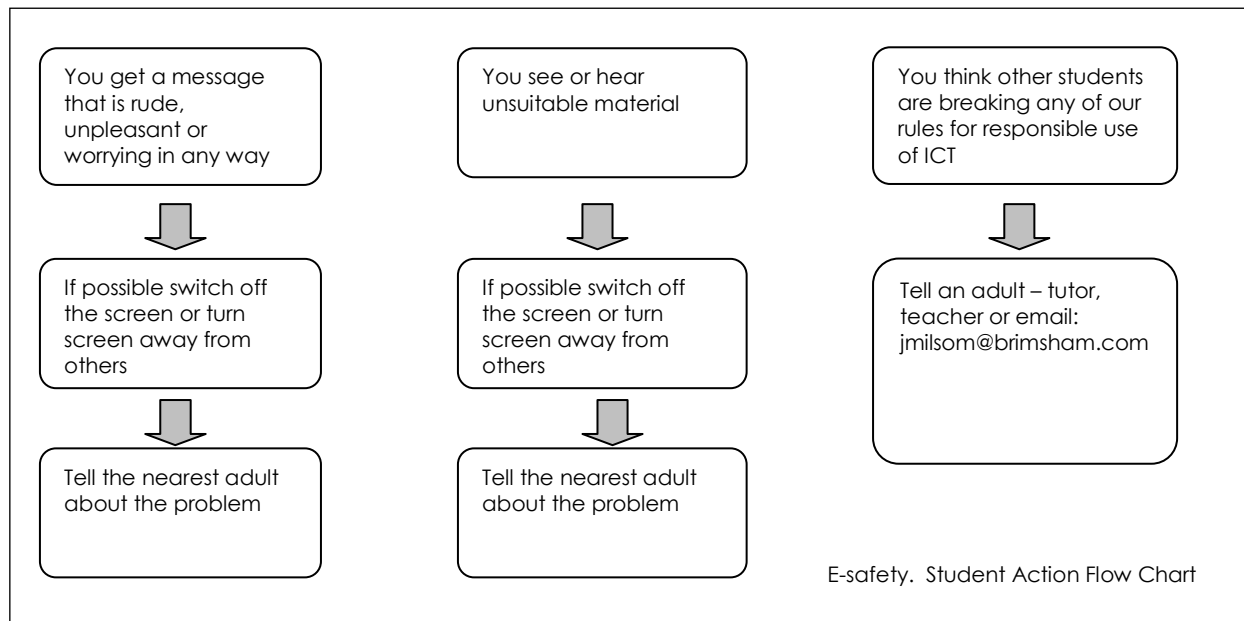
User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by ICT technical group meetings.

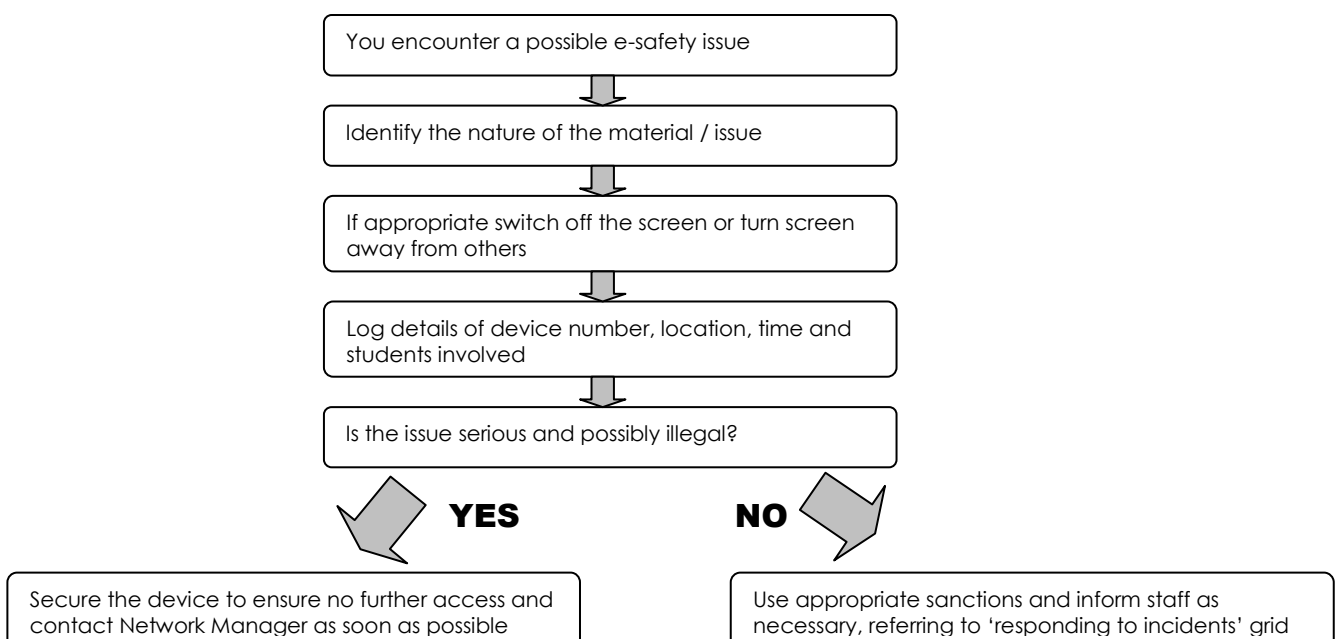
This policy will be regularly annually in response to changes in guidance and evidence gained from the logs.

## Appendix 6 – Action flow charts

It is important that students are clear as to the correct course of action to take to protect both themselves and others in the event of encountering an e-safety issue. The flow chart below outlines the course of action to be taken by students and is intended to make it clear to students in an easy to understand way what they should do in the event of an e-safety incident, it does not replace the detailed action as described in the student grid in the 'responding to incidents of misuse' section of the policy. The flow chart is to be displayed in all ICT rooms and will be used by ICT teachers to refer to as part of the ICT taught curriculum.



All staff and volunteers need to be clear as to the correct course of action if they encounter an e-safety issue. The 'responding to incidents of misuse' section of the policy provided detail on the course of action needed for each type of incident. This flow chart is intended to help staff understand how to deal with the particular case of encountering an e-safety incident during a lesson or when in contact with students as a part of their daily work.



## Appendix 7 – Rules for Responsible use of ICT

Students need a clear and understandable set of rules to help them understand how to be responsible users and to stay safe whilst using the Internet and other communications technologies. These rules are not a replacement of the Acceptable Use Agreement but rather are a means of enabling pupils to understand the agreement better.

This set of rules is to be displayed in all ICT rooms and will be used by ICT teachers to refer to as part of the ICT taught curriculum.

### **Brimsham Green School**

#### **Rules for Responsible Internet and Network Use**

The school has installed computers with Internet access to help our learning. These rules will keep you safe and help us to be fair to others.

When I use communications technology I agree to the following:-

1. I will only access the school system with my own user name and password, which I will keep secret.
2. I will use the computers for school work and homework only.
3. I will only e-mail people I know, or my teacher has approved.
4. The messages I send will be polite and responsible. I will not use ICT to bully or harass others.
5. I will not give my home address, telephone number, e-mail address, or any other personal details, or arrange to meet someone, unless my teacher has given permission.
6. I will report to an adult any unpleasant or inappropriate material or messages.
7. I understand that the school will check my computer files, will monitor the Internet sites I visit and all emails I send and receive.
8. I will not attempt to view, access, download or distribute unsuitable material.
9. I will not attempt to change the configuration of any school computer or install software.
10. I will not take or distribute images of anyone without their permission.
11. I will not use my personal devices (mobile phone etc) in school without permission

I understand that Brimsham Green School reserves the right to withdraw Internet or computer access.

## Appendix 8 - Legislation

The legislation that forms the legal basis for much of this document is as follows:

### Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

### Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

### Freedom of Information Act 2000

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

### Communications Act 2003

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.

### Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

### Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
  - Ascertain whether the communication is business or personal;
  - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

#### **Trade Marks Act 1994**

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

#### **Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

#### **Telecommunications Act 1984**

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

#### **Criminal Justice & Public Order Act 1994**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

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

#### **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.

## Protection from Harrassment 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.

## Protection of Children Act 1978

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

## 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.

## Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

## Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

## Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

## **The Education and Inspections Act 2006**

Empowers Headteachers, 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.