REDLAND GREEN SCHOOL
BRISTOL

E-SAFETY POLICY

1 INTRODUCTION

1.1 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. Redland Green School has made a significant investment both financially and physically to ensure these technologies are available to all learners.

1.2 The benefits are perceived to "outweigh the risks." Redland Green School will ensure that statutory obligations are met to ensure that students are safe and are protected from potential harm, both within and outside school. This policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

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

1.4 The Education & 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 are linked to membership of the school.

1.5 Staff can access the Schedule for Monitoring & Review here.

2 AIMS

2.1 Students will receive an education that will provide the opportunity to reflect on e-safety within their lessons, mentor programme and assembly programme. Parents will be signposted to key areas of interest through the e-safety blog and at least one opportunity to receive some face-to-face guidance. Teaching and support staff will be signposted to the e-safety blog as well as receiving regular direct guidance via email as and when issues become prominent. Teaching staff will be guided towards ways to engage the e-safety message with their students at regular points within the year. Governors will, as a minimum, have opportunities to engage with whole school e-safety as part of their on going training.

2.2 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.

2.3 Within the policy clear guidance is given as to the actions that should be taken if an e-safety concern is raised. This sits firmly within the broader safeguarding umbrella. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

3 ROLES & RESPONSIBILITIES

3.1 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 Governors receiving regular information about e-safety incidents, and monitoring reports.

3.2 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.

3.3 The Headteacher is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable continuing professional development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

3.4 The Headteacher and another member of the Strategic Leadership Team (SLT) 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.

3.5 The SLT will receive regular monitoring reports from the E-Safety Officer; a termly meeting will also take place between the E-Safety Officer and the Designated Child Protection Officer (DCPO).

3.6 The **E-Safety Officer** within the safeguarding team**:**

- 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/external agencies where appropriate
- Reviews the safeguarding log with regard to e-safety concerns
- When requested, attends meetings of the Governing Body
- Reports regularly to the SLT
- 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 IT Support Team staff
- Receives reports of e-safety incidents and where appropriate, through the Heads of House, this will be recorded on the safeguarding log
- Provides advice and training for staff where appropriate
- Ensures that teaching staff are well prepared to inform their curriculum with reference to e-safety issues as appropriate; all teaching staff should feel enabled to include e-safety advice within their curriculum
- Monitors the delivery of the e-safety curriculum to ensure it is effective and meets the needs of students and reflects changes in technology
- Liaises with the IT Support Team Leader to ensure that all measures are taken to maintain a secure ICT infrastructure

3.7 The **IT Support Team Leader** 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

- That users may only access the school's networks through an enforced password protection policy

- That s/he 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 IT Support Team Leader in the configuration, operation and maintenance of the school systems to ensure they are not open to misuse

3.8 **Teaching and Support Staff** are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the school's E-Safety Policy and practices

- They have read, understood and signed the school Staff Acceptable Use Policy Agreement

- They report any suspected misuse or problem to the E-Safety Officer or other staff as shown in the grid 'responding to incidents of misuse – students'

- Digital communications with students (email/Google Apps/any future Virtual Learning Environment (VLE)/voice/website) should be on a professional level

- Students understand and follow the school's E-Safety Policy and Acceptable Use Policy Agreement

- 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

3.9 The **Child Protection Officers** 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

3.10 **Students:**

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy Agreement, 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

3.11 **Parents** 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 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 will be responsible for:

- Endorsing the Student Acceptable Use Policy Agreement

- Accessing the school website and when available, VLE/Google Apps content and on-line student records in accordance with the schools Acceptable Use Policy Agreement

4 EDUCATION & TRAINING

4.1 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. Students need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

4.2 E-safety education will be provided in the following ways:

- All students are required to agree to the school's Acceptable Use Policy Agreement

- Planned e-safety programme will be provided as part of ICT/PHSE/Citizenship/APEX lessons and will be regularly revisited; this will cover both the use of ICT and new technologies in school and outside school

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities

- Students should be taught in all lessons to be critically aware of the materials/content they access to on-line and be guided to validate the accuracy of information

- Students should be helped to understand the need for the student Acceptable Use Policy Agreement 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

4.3 PARENTS

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 their 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).

4.4 The school will therefore seek to provide information and awareness to parents through:

- Blog, Letters, newsletters, web site and information evenings
- Reference to the South West Grid for Learning's (SWGfL) Safe website

4.5 **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's E-Safety Policy and Acceptable Use Policies. This will be integrated within the broader safeguarding training
- This policy and its updates will be presented to, and discussed by staff, during INSET days; this will be integrated within the broader safeguarding updates
- The E-Safety Officer will provide advice/guidance/training as required to individuals

4.6 **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 (LA)/National Governors Association/ SWGfL or other relevant organisation
- Participation in school training/information sessions for staff or parents

5 ICT INFRASTRUCTURE, EQUIPMENT, FILTERING & MONITORING

5.1 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.

5.2 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 e-safety policy and guidance.

5.3 There will be regular reviews and audits of the safety and security of school ICT systems; this will take place at fortnightly IT Support Team meetings.

5.4 Servers, wireless systems and cabling must be securely located and physical access restricted.

5.4 All users will have clearly defined access rights to school ICT systems.

5.5 All users will be provided with a username and password by the ICT Technician in charge of user administration, under the guidance of the IT Support Team Leader, who will keep an up to date record of users and their usernames.

5.6 The "administrator" passwords for the school ICT system, used by the IT Support Team Leader will be available to the Headteacher or other nominated senior leader and kept in the school safe.

5.7 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.

5.8 The school maintains and supports the managed filtering service provided by the LA. In addition, the school has provided enhanced user-level filtering through the use of the "Netsweeper" filtering programme.

5.9 The IT Support Team Leader only will control the filtering system. In the event of the IT Support Team Leader 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.

5.10 Any filtering issues should be reported immediately to the LA.

5.11 Requests from staff for sites to be removed from the filtered list will be considered by the IT Support Team Leader and E-Safety Officer. If the request is agreed, this action will be recorded.

5.12 School IT Support Team 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 Agreement.

5.13 Remote management tools are used by staff to control workstations and view users activity.

5.14 An appropriate system is in place for users to report any actual/potential e-safety incident to the IT Support Team Leader and E-Safety Officer.

5.15 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.

5.16 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 IT Support Team Leader, administer such access.

5.17 Users will not be allowed to download executable files with the exception of IT Support Team staff and the Head of ICT.

5.18 Users will not be allowed to install software onto any school device, with the exception of IT Support Team staff and the Head of ICT, all requests for such installation will be made through the IT Support Team Leader.

5.19 The school infrastructure and individual workstations are protected by up-to-date virus software.

6 CURRICULUM

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

7 USE OF DIGITAL & VIDEO IMAGES: PHOTOGRAPHIC, VIDEO

7.1 The use of digital images can bring significant benefits to a range of educational experiences when utilised under the following guidelines.

7.2 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.

7.3 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.

7.4 Students must not take, use, share, publish or distribute images of others without their permission.

7.5 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.

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

7.7 Students' work can only be published with the permission of the student and parents.

8 DATA PROTECTION

8.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and in line with the school's Data Protection & Personal Data Handling Policy.

9 COMMUNICATIONS

9.1 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 (email, chat, via Google Apps/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

10 RESPONDING TO INCIDENTS OF MISUSE

10.1 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:

10.2 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

staff should consult the school's Internet Safety Protocol flow chart and the E-Safety Incident flow chart, 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.

10.3 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 & 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.

10.4 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.

10.5 The Student and Parents Acceptable Use Policy Statements appear in Student Planners and are linked here. Students agree to an electronic version at the start of Term 1 annually.

10.6 The Staff Acceptable Use Policy Agreement is linked here.

Agreed by Staff	Agreed by Pupils	Agreed by Governors	Review Schedule	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed
02 DEC 2014	02 DEC 2014	02 DEC 2014	ANNUALLY				
Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed

APPENDIX 1 – CURRICULUM OUTLINE

ICT LESSONS

All Key Stage 3 (KS3) students at Redland 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.

Issues of plagiarism and copyright infringement are integral to the GCSE syllabus content undertaken by all students in Years 10 and 11.

APEX/PSHE/CITIZENSHIP LESSONS

The role that the online world plays in a range of issues are explored and developed through this curriculum area.

ASSEMBLIES

Assemblies will be used throughout the year to highlight the importance of e-safety. There will be an assembly to support Safer Internet Day every February. Additionally, issues related to e-safety and cyber-bullying will feature as part of a broader safeguarding agenda.

APPENDIX 2 – 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 the school.

RESPONSIBILITIES

The responsibility for the management of the school's filtering policy will be held by the IT Support Team Leader. S/he will manage 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 LA filtering service must:

- Be logged in change control logs
- Be reported to a second responsible person (member of SLT)

All users have a responsibility to report immediately to the IT Support Team Leader 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 Policy 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 IT Support Team Leader who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at LA level, the IT Support Team Leader will address this.

AUDIT & REPORTING

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

- The Head of ICT
- IT Support Team meetings
- SLT
- Governors
- The LA 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 3 – 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 Data Protection & Personal Data Handling 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 Google Apps, email and any future 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 IT Support Team Leader.

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 IT Support Team Leader and will be reviewed, at least annually, by SLT.

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 eg 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 IT Support Team Leader must also be available to the Headteacher or other nominated senior leader and kept in the school safe.

AUDIT, MONITORING, REPORTING & REVIEW

The IT Support Team Leader will ensure that full records are kept of:

- User Ids

- 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. Similarly, the school’s auditors may request 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 the SLT at appropriate delegated meetings.

APPENDIX 4 – 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.

E-Safety: Student Action List/Flow Chart

You see or hear unsuitable material

1. Switch off the screen
2. Tell the nearest adult about the problem

You get a message that is rude, unpleasant or worrying in any way

1 Switch off the screen
2 Tell the nearest adult about the problem

You think other students are breaking any of our rules for responsible use of ICT

1 Tell an adult – email, teacher or email designated member of SLT/Head of ICT
2 You can make a confidential report via the RGS Whisper button; in order to investigate issues it is important that you give us as much detail as possible

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 provides details 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.

E-Safety: Staff Action List/Flow Chart

You encounter a possible e-safety issue

1 Identify the nature of the material/issue
2 If appropriate, switch off the screen or turn screen away from others
3 Log details of device number, location, time and students involved
4 Is the issue serious and possibly illegal?

YES: Secure the device to ensure no further access and contact IT Support Team Leader as soon as possible

NO: Use appropriate sanctions and inform staff as necessary, referring to 'responding to incidents' grid

APPENDIX 5 – 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 Policy Agreement but rather are a means of enabling students 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.

RULES FOR RESPONSIBLE INTERNET & 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 schoolwork 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.

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

APPENDIX 6 – 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 personal 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 & 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, sounds, moving images, TV broadcasts and other media (eg 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 & 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 that is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

PROTECTION FROM HARASSMENT ACT 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which s/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 her/him is guilty of an offence if s/he knows, or ought to know, that her/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 a computer means that the person has 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 a person's 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 that is threatening. Like the Racial & Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence. (Children, Families & Education Directorate, page 38 April 2007).

OBSCENE PUBLICATIONS ACT 1959 & 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 & INSPECTIONS ACT 2006

This act 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.