



## CLIFTON COLLEGE

Title/Date	E-Safety Policy (Upper School) June 2011
Background	<p>The School is sufficiently flexible to manage new and emerging technologies; it encourages students to use new technology, which includes electronic tools or other such electronic devices, as they have important educational and social benefits. Our policy aims to balance the desirability of fully exploiting the vast educational potential of new technologies with providing safeguards against risks and unacceptable material and activities.</p> <p>This Policy considers all technological appliances used by pupils and employees and includes: both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams and digital video equipment); and technologies owned by pupils and employees, but brought onto school premises (such as laptops, mobile phones, 'smart' phones, personal digital assistants (PDAs), and portable media players).</p> <p>Although pupils may be trusted by their parents with regard to private internet use, the School has a legal obligation to safeguard all pupils. Parents need to be reassured that their child is not able to access material deemed unsuitable and/or in contravention of the school's Electrical Device Acceptable Use Agreement.</p>
Aims/Targets	<ul style="list-style-type: none"> <li>• To protect and safeguard pupils in their use of ICT and e-technology.</li> <li>• To ensure that pupils are ICT literate and can use the facilities to ensure that their educational provision is enhanced to the maximum.</li> <li>• To raise awareness of and counter instances of cyber bullying. This includes bullying via text message, via instant-messenger services and social network sites, via email, and via images or videos posted on the internet or spread via mobile phone. It can take the form of any of the previously discussed types of bullying, i.e. technology can be used to bully for reasons of race, religion, sexuality, disability, etc. (<i>See appendix to Anti Bullying Policy regarding Cyber Bullying.</i>)</li> <li>• Appropriate and very careful use of social networking sites or personal web pages</li> <li>• Concerns regarding internet chat rooms which are geared towards teenagers. These are known for explicit sexual talk/obscene language and this is likely to attract online predators. Internet offenders target teenagers willing to talk online about sex, will manipulate young people into criminal sexual relationships by appealing to the desire of youth to be appreciated, understood, take risks and find out more about sex.</li> </ul>
Rationale/Issues	<p><u>New Technology</u> Pupils are keen to grasp the opportunities offered by new technology and their availability, portability, miniaturisation and use of sophisticated electronic devices. However, as with any new technology, there are associated risks which include the following: exposure to inappropriate material, physical danger, online/cyber bullying, legal and commercial issues, personal financial gain, gambling and addictive behaviour.</p> <p><u>Security &amp; Individual responsibility</u> The existence of the many and various forms of electronic devices and equipment, in any environment, raises issues of security and personal responsibility, not only in terms of its appropriate use but also for its safe keeping. The School does not accept responsibility for, nor is insured against theft, loss or damage of any pupils' personal property, including electronic devices.</p>
Procedures and practices	<p>The School provides every pupil with internet access and access to the school's own network through connections in all the houses. This service is provided free of charge and parents are actively discouraged from allowing their son/daughter to have access to devices which will allow them to circumvent the school's network system and the safety that this affords. Accordingly, pupils are not allowed the use of technology which would allow them access to the internet by means other than through the school's ICT system; exception being voice based communication from phones, this does not include visual or video communication.</p> <p><b>Measures in place to support the policy:</b></p> <ol style="list-style-type: none"> <li>1. <b>The Electrical Device Acceptable Use Policy</b> protects all parties by clearly stating what is acceptable and what is not. Pupils and their parents/guardians are expected to sign up to this before access can be given to the school's ICT facilities.</li> <li>2. <b>Induction.</b> All pupils joining the School are inducted in appropriate use of the school's ICT facilities and other aspects of this policy.</li> <li>3. <b>Education</b> <ul style="list-style-type: none"> <li>• All pupils joining the school in the 3<sup>rd</sup> Form receive ICT lessons. A key component of these lessons is to achieve a great understanding of the important issues of e-safety contained within this policy.</li> <li>• PSHE lessons address cyber-bullying and safe use of the internet. The programme discusses the acceptable use of ICT, including computers not linked to the School Network, mobile phones, and camera phones. <i>See the School's Anti Bullying Policy</i></li> </ul> </li> <li>4. <b>Monitoring</b> The school will exercise its right to monitor the use of computer systems, including the monitoring of internet use, interception of e-mails and the deletion of inappropriate materials at all times. In circumstances where the</li> </ol>

	<p>school believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the school reserves the right to inform appropriate authorities and provide documentary evidence. The computer network is owned by the school and may be used by pupils to advance and extend their knowledge and understanding.</p> <p>Pupils should be aware that computer/mobile phone memory, e-mails and other forms of electronic information storage and communication (including any external storage media which pupils bring into the School) may be scrutinised for the purposes of safeguarding or promoting a child's welfare or maintaining and promoting the well being of the school community as a whole. This is done in accordance with the <i>Protocol for managing, testing and investigating the security of the IST system</i>.</p> <p>Although all staff and pupils at Clifton College are expected to use ICT responsibly and receive specific education to define and encourage responsible use, the College recognises that it has a responsibility to counter any attempts at irresponsible behaviour which may still arise. Thus:</p> <p>The School's ICT system is monitored and managed in a number of ways designed to inhibit abuses, specifically:</p> <ul style="list-style-type: none"> <li>• Code of Conduct: All users agree to abide by the code of conduct and other published rules</li> <li>• User Logons and Passwords – all users have their own private logons and password. Users who are careless or negligent with their passwords are punished appropriately.</li> <li>• Access rights to confidential data – the ICT staff work hard to ensure that all users understand that confidential data must be stored in folders controlled by appropriate access rights.</li> <li>• Web Filtering – the School subscribes to a reputable service (MessageLabs) that maintains an on-line database that categorises websites. Some categories are banned permanently, some are restricted to adults only and some are restricted to certain groups.</li> <li>• Control of Leisure time – pupils are restricted from using leisure sites during working hours. All Internet use is switched off at 11 pm (earlier for younger pupils).</li> <li>• Computer Logs – all user logon and logoff activity is logged. All website requests are logged and users are taught this.</li> <li>• Social Networking sites – access to these is limited to certain times of the day.</li> </ul> <p><b>5. Expectations of Pupils and Parents beyond the School.</b></p> <p>When a pupil is at home, families bear responsibility for the guidance of their children. The School expects the use of ICT by its pupils, even when at home, to comply with the School's stated ethos, accord with the College Rules, and honour the agreement they sign permitting their use of ICT at the School. Material downloaded in the home, posted in cyber-space from a home computer, or transmitted to a mobile phone when a pupil is at home, can impact significantly upon the life of pupils and other members of the School community. Thus the School requires the parents/guardians of pupils enrolled at Clifton to cooperate with the School in the education of their children in the use of ICT.</p> <p><b>6. Sanctions</b></p> <ul style="list-style-type: none"> <li>• Most initial offences will be dealt with by the HoM (often in conjunction with the Director of Office Services) and the removal of computer/mobile phone access may result. In such circumstances parents/guardians will be notified.</li> <li>• More serious offences or repeated abuse of ICT by a College pupil will be dealt with by the Deputy Head (Pastoral). The removal of computer/mobile phone access may result and other sanctions may also be applied. In such circumstances the Deputy Head (Pastoral) will normally write to a pupil's parents/guardians.</li> <li>• Under circumstances when abuses of ICT constitute illegal activity the Head Master will interview the pupil with his/her parents (or guardians). Sanctions applied will be proportionate to the offence committed.</li> <li>• The school's Child Protection Officer should be informed and procedures will be followed in circumstances when there are concerns over safeguarding pupils and child protection issues.</li> <li>• The School is entitled to take disciplinary action if the reputation of the School is adversely affected by pupils' actions.</li> </ul> <p><b>7. Pupil Input</b></p> <p>Pupils can voice their own views on the school's ICT provision through both the Student Council and the individual House ICT Representatives.</p>
Links with other policies and documents	School rules; Anti-Bullying Policy; Electrical Device Acceptable Use Agreement; Safeguarding and Protecting Children Policy; Protocol for managing, testing and investigating the security of the IST system.
Implementation By whom to whom and how disseminated	All Staff should be aware of and implement this policy. HoMs, House staff, Marshal, DHs, HM and if necessary parents and Police Published in Staff handbook, HoMs handbook Parents are apprised of these regulations via the Parents Handbook.
Review	After any such incident or June 2012