Castilion Primary School

E-Safety Policy

(Based on Hertfordshire Model, LGfL, SWGfL, Bristol City Council, Becta guidance and Government advice on the PREVENT strategy.)

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Learning Platforms and Virtual Learning Environments;
- Email and Instant Messaging;
- Chat Rooms and Social Networking (Facebook, What‟s App, Skype etc);
- Blogs and Wikis;
- Podcasting;
- Video Broadcasting;

- Music Downloading;
- Gaming;
- Online gaming;
- Mobile/ Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality (e.g. tablets).

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Castilion School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) include both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

E-Safety and the PREVENT strategy

HM Government has published guidance for authorities, including schools, on their responsibilities under the Counter-Terrorism and Security Act, which came into effect on 1 July 2015. Under the Act, schools and other authorities have a duty to 'have due regard to the need to prevent people from being drawn into terrorism'.

'Prevent' is a government strategy designed to stop people becoming terrorists or supporting terrorist or extremist causes. The Prevent strategy covers all types of terrorism and extremism, including the extreme right wing, violent groups and other causes.

From July 2015 all schools (as well as other organisations) have a duty to safeguard children from radicalisation and extremism. This means that we have a responsibility to protect children from extremist and violent views in the same way that we protect them from other dangers. Importantly, we can provide a safe place for pupils to discuss these issues in order for them to better understand how to protect themselves.

Our policy and practice ensures that:

- Children are safe from terrorist and extremist material when accessing the internet in school, due to the establishment of appropriate levels of filtering (internal school and / or external (lgfl).
- We ensure pupils cannot access dangerous content, or be contacted online by extremist groups.
- General internet safety is embedded in our school's computing curriculum.
- Every teacher is aware of the risks posed by the online activity of extremist and terrorist groups.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-coordinator in our school is Miss Clinch who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-coordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Leadership and Governors are updated by the Head / e-Safety coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (see appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection; health and safety; home–school agreements; and behaviour/pupil discipline (including anti-bullying) and PSHE.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of updates at staff meetings and correspondence from co-ordinator;
- New staff receive information on the school's acceptable use policy as part of their induction;
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community;
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.
- Managing the school e-Safety messages
- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used;
- The e-Safety policy will be introduced to the pupils at the start of each school year;
- E-Safety posters will be prominently displayed.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe that it is essential for e-Safety guidance to be given to our pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities for its promotion.

- The school has a framework for teaching internet skills in Computing / PSHE lessons;
- The school provides opportunities within a range of curriculum areas to teach about e-Safety including the potential dangers of social network sites;
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum;

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which, while it may limit what they want to do, also serves to protect them;
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities;
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent / carer; teacher/ trusted staff member, or an organisation such as Childline or the CEOP report abuse button.
- Children are kept safe from terrorist and extremist material when accessing the internet in school, by the establishment of appropriate levels of both school and/or external (lgfl) filtering.
- We ensure that pupils cannot access dangerous content, or be contacted online by extremist groups.
- General internet safety is embedded in our school's computing curriculum.
- Every teacher is aware of the risks posed by the online activity of extremist and terrorist groups.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school‟s e-Safety policy;
- Users will be provided with an individual network, email and Learning Platform log-ins and usernames ;
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or the Learning Platform, including ensuring that passwords are not shared. Individual staff users must also make sure that workstations are not left unattended unless are locked;
- In our school, all ICT password policies are the responsibility of Miss Clinch.

Data Security

- The unauthorised accessing and inappropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008).
- Staff are aware of their responsibilities when accessing school data. Level of access is determined by the HT;
- Data protection and anti-virus software on PCs is used to protect data.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the London Grid for Learning (LGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school will provide supervised access to Internet resources (where reasonable) through the school's fixed & mobile internet technology;
- Staff will preview any recommended sites before use;
- Raw image searches are discouraged when working with pupils;
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any such work. All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegally obtained software from other sources;
- All users must observe copyright of materials from electronic resources.
- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to http://cms.lgfl.net/web/lgfl/homepage;
- Castilion School is aware of its responsibility under current legistlation when monitoring staff communication and takes into account: The Data Protection Act 1998; The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998;
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required;
- The school does not allow pupils access to internet blogs;
- If staff or pupils discover an unsuitable site, it must be closed immediately and the incident reported to the e-Safety co-ordinator;
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines;
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses e.g. making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility, to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media, it must be given to the teacher for a safety check first;
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher/ICT subject leader.
- If there are any issues related to viruses or anti-virus software, the ICT coordinator should be informed who will in turn inform the technician and technical support team for assistance.

Managing other Web 2 technologies

Web 2 (user-generated content), including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. At present, the school endeavours to deny access to social networking sites to pupils within school other than the facilities provided by the VLP.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are;

- Pupils are taught to avoid placing images of themselves (or details within images that could give background information) on such sites and to consider the appropriateness of any images they do post due to the near – impossibility of removing an image once uploaded;
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests, diary plans etc.);
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals;
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online;
- Our pupils are asked to report any incidents of cyber-bullying to the school;
- If children reveal any level of sexual and/or inappropriate knowledge accessed from the computer/Internet, the teacher must immediately report this to the designated Child Protection Officer;
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the DB Primary or other systems approved by the Headteacher;
- It is forbidden for any staff member to accept a current pupil or parent as a 'friend' on Facebook or any other social networking site – failure to comply will lead to disciplinary action.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. These generally allow internet access and thus open up the risk of misuse. associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device;
- This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer;
- Pupils are not allowed to bring personal mobile devices/phones to school without the permission of the class teacher. Any phones then brought to school must have only basic call and text functions and no camera or Internet access facility. They should be stored securely in the class cupboard at the start of the day and returned to the owner as he / she leaves.
- The school is not responsible for the loss, damage or theft of any personal mobile device;
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed;
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community;
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used;
- In cases where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, e-mail can offer significant benefits including: direct written contact between schools on different projects (staff based or pupil based), within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good „netiquette".

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed;
- Staff must use the official school e-mail (StaffMail) system for work e-mails
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. If necessary, email histories can be traced. This should be the account that is used for all school business;
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses;
- E-mail sent to an external organisation should be written carefully and checked before sending, in the same way as a letter written on school headed paper;
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account;
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (or 'netiquette') particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communications. They should not arrange to meet anyone without specific permission and should virus-check all attachments and shouldn't open e-mails from an unknown or untrusted source.
- Pupils must tell a teacher/ trusted adult immediately if they receive an offensive e-mail. On DB, this would be done by 'blowing the whistle'
- Staff must inform (the e-Safety co-ordinator and Headteacher) if they receive an offensive e-mail; on the school system.
- Pupils are introduced to e-mail as part of the Computing Scheme of Work.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and are therefore easy to misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment;
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on field trips. However, with the express permission of the Headteacher, images can be taken provided that they are transferred immediately and solely to the school's network and deleted from the staff device;
- Pupils are not permitted to use personal digital equipment, (including mobile phones and cameras) to record images of the others. This includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided that they are transferred immediately and solely to the school's network and deleted from the pupil's device.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site;
- in the school prospectus, newsletter and other printed publications that the school may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in the school's communal areas;
- in display material that may be used in external areas, i.e. exhibitions promoting the school;
- in general media appearances, e.g. local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents / carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Only the Web Manager has authority to upload to the site.

Storage of Images

- Images / films of children are only to be stored on the school's equipment and website;

- Pupils and staff are not permitted to use personal portable media (USB sticks etc.) for the storage of images without the express permission of the Headteacher;
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network;

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator;
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator and, depending on the seriousness of the offence, investigation by the Headteacher / LA; immediate suspension possibly leading to dismissal and the involvement of police for very serious offences (see flowchart);
- Users are made aware of sanctions relating to misuse or misconduct. All staff are aware of the policy and the children have all signed an acceptable use policy.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message to parents for all pupils and this in turn should aid the establishment and future development of the school's e-Safety rules. However, Staff are aware that some pupils may require additional teaching such as reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents / carers to be fully involved with promoting e-Safety both in and outside of school. We regularly consult and discuss e-Safety with parents / carers and seek to promote a wide understanding of both the benefits and risks related to the use of ICT.

Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain e.g. on school website.

The school disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website / Learning Platform postings
- Newsletter items
- **Reviewing this Policy**

There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them.

This policy will be reviewed every 24 months and consideration given to the implications for future whole - school development planning.

The policy will also be amended if new technologies are adopted or Central Government changes the orders or guidance in any way.

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct / Primary Pupil Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to it at all times. Any concerns or clarification should be discussed with the school e-Safety coordinator.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998 - The Act requires anyone who handles personal information to comply with important data protection principles regarding personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing. http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to e-Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

18

 access to computer files or software without permission (for example using another person's password to access files);

 unauthorised access, as above, in order to commit a further criminal act (such as fraud);

 impair the operation of a computer or program.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Education and inspections act 2006

An Act to make provision about primary, secondary and further education and about training; to make provision about food or drink provided on school premises or in connection with the provision of education or childcare; to provide for the establishment of an Office for Standards in Education, Children's Services and Skills and the appointment of Her Majesty's Chief Inspector of Education, Children's Services and Skills and make provision about the functions of that Office and that Chief

Inspector; to provide for the amendment of references to local education authorities and children's services authorities; to amend section 29 of the Leasehold Reform Act 1967 in relation to university bodies; and for connected purposes.

Policy agreed: 30.11.15

Policy reviewed: 30.11.17

Chair of Governors (sig):