



BISHOP VESEY'S GRAMMAR SCHOOL
E-Safety Policy
Whole school policy

Staff covered by this procedure:	Whole school policy (staff and students)
Review prepared by:	Review 1: Kate Steadman – Assistant Headteacher June 2015 Review 2: Dominic Robson – Headteacher November 2016
Review approved by and date:	Review 1: 1 June 2015 HR Committee Review 2: 1 November PPD Committee & June 2016 Learning & Teaching Committee
Staff consultation period:	June 2015. No further consultation in Autumn 2016 – no changes required.
School adoption date (for reviewed policy):	Review 1: 1 June 2015 Review 2: 1 November 2016
School's next review date/by whom:	October 2017 PPD Committee & Learning & Teaching Committee – annual review
Signed by Chair of PPD Committee & date:	
Signed by Chair of Learning & Teaching Committee & date:	

Our e-Safety Policy has been written by Kate Steadman Assistant Head Teacher Teacher i/c Safeguarding and Child Protection. It has been agreed by the Senior Leadership Team and approved by Governors. It will be reviewed annually.

Context:

Safeguarding

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by all users of the school's ICT systems.

Effective and safe use of digital resources

Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

The Green Paper *Every Child Matters* and the provisions of the *Children Act 2004*, *Working Together to Safeguard Children* and the *Keeping Children Safe in Education (2015)* state that individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Most of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, the internet is used for grooming children and young people with the ultimate aim of exploiting them sexually; ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour; and there are increasing numbers of children making and sending partially naked, nude or sexualised images of themselves via the internet or mobile technology.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging including the use of simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones & smart TVs with e-mail and web functionality.

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- An E-Safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Head teacher ensures the policy is implemented.

Responsibility for e-Safety has been designated to the DSL, Kate Steadman, a member of the Senior Leadership Team.

The DSL ensures they keep up to date with e-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection and has gained a qualification in E-safety from EPICT. She has also attended a CEOP course. The DSL ensures the Head, Senior Leadership and Governors are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following E-Safety procedures. Central to this is fostering an open culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff, teaching and non-teaching, are reminded / updated about E-Safety matters at least once a year and new staff will receive induction about the school's E-safety policy.

At Bishop Vesey's, E-safety is incorporated into an awareness programme in Year 7 and into form period materials across years 7-11. Pupils across all three Key Stages are educated about safe and responsible use of ICT through assemblies including Internet Safety Day. Pupils know how to control and minimise online risks and how to report a problem. On the school website are guides for pupils and parents regarding aspects of safe and responsible use of ICT.

Parents also receive a presentation on how to protect their children online through the School's annual Welcome Evenings. This presentation is also on the school's website. Parents are also contacted about E-safety issues either via the school communications system or post. Parents/guardians/carers have signed and returned an e-safety/AUP form.

4. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that

unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by form tutor / Head of Year / DSL / Head teacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to National College for Teaching and Leadership (staff only) / Police.

The DSL is the first point of contact for any complaint. Complaints related to Child Protection are dealt with in accordance with national Child Protection procedures. Any complaint about staff misuse is referred to the Head teacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.