	Bishop William Ward Primary School
	E-safety Policy

Introduction

ICT (Information and Communication Technology) 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 on the use of these technologies in order to equip our children with the skills to access life-long learning.

Technology and communications are rapidly changing and becoming more sophisticated. With this change comes new ways of being unsafe and feeling threatened. E-safety has become a very important issue that is essential to address in school throughout different areas of the curriculum, to ensure that all children and adults remain safe and in control when using technology. This could be either computers and having access to the internet or through mobile devices, such as phones and tablets.

At Bishop William Ward we understand the responsibility to educate our pupils in 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.

Bishop William Ward's E-safety Policy will operate in conjunction with other policies including those for Pupil Discipline and Behaviour and the ICT Curriculum.

Aims

We aim to help every pupil and adult to:
·   Feel safe and confident when using new technologies.
·   Know who to speak to when they feel unsafe.
·   Know how to report any abusive behaviour.
·   Know how to use the internet correctly, without misuse.
·   Stay in control and keep personal information private.
·   Know how to take the necessary measures to block and delete accounts, messages and people.

 Roles and Responsibilities

All the adults and pupils that are involved in the life of the school have roles and responsibilities that are associated with E-safety.

Governors

The Governors are responsible for the approval of the E-safety Policy and reviewing the effectiveness of it regularly. Regular meetings and information will be provided to the Governors so they are able to make the correct recommendations. They will also be able to carry out regular monitoring of E-safety incident logs when required.

Headteacher and Senior Leadership

The Headteacher is responsible for ensuring the safety, including E-safety, of the members of the school community. However, the day to day managing of E-safety will be delegated to the Computing (curriculum) Co-ordinator.

The Headteacher and Senior Leadership Team:
· are responsible for ensuring that all staff and the E-safety Co-ordinator receive correct and suitable Continuing Professional Development (CPD).
· will ensure that there is a system in place to monitor the usage of internet and other technologies and that the person who carries out the internal E-safety monitoring receives support and is also monitored
· will ensure that they receive regular updates from the E-safety Co-ordinator.
· are to ensure they know the correct procedures that need to be followed when a serious allegation has been made by a child or one that is in regards to a member of a staff.

E-safety Co-ordinator

The E-safety Co-ordinator:
· will take day to day responsibility for E-safety issues
· has a leading role in establishing and reviewing the school E-safety policies/documents.
· ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
· will provide training and advice for all staff.
· will liaise with school ICT technical staff.
· receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments.

Technical Staff

The ICT Technician and ICT (technical) Co-ordinator are responsible for ensuring:
· that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
· that users may only access the school's networks through properly enforced password protection.
· that they keep up to date with relevant E-safety technical information and guidance in order to carry out their role effectively.
· that virus protection is implemented and up dated regularly.

Teaching and Support Staff

Teaching and Support Staff are responsible for-
· Ensuring they stay up to date with current E-safety matters and policies and practice.
· Making sure that they have read, understand and carry out the Acceptable Use Policy (AUP).
· reporting any misuse or problems to the E-safety Co-ordinator/Headteacher for further investigation.
· Ensuring that any digital communications with pupils (email, Learning Platform) should be strictly professional and only carried out using school systems.
· Embedding E-safety issues throughout the curriculum.
· Ensuring that that pupils follow the AUP and E-safety policy.
· Being aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and monitoring their use, implementing current school policies with regard to these devices.

Child Protection Officer

The Child Protection Officer needs to ensure that they are fully trained in E-safety issues and are aware that serious child protection issues could occur due to:
· Cyber-bullying
· Sharing of personal data
· Inappropriate online conduct with adults/strangers
· Potential or actual incidents of grooming

Pupils

Pupils and students are responsible for:
· Knowing and acting accordingly to the db Primary Home-School agreement.
· Knowing the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to report them.
· Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying.
· Understanding that the E-safety policy also covers their actions out of school, if related to their membership of the school.
· Agree to and sign the db Primary Home-School Internet and Learning Platform User Agreement.

Parents/Carers
Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They will be provided with a basic E-safety policy within their admissions pack, and will be expected to sign the Bishop William Ward Internet & E-communications Permission form. In addition to this, they will be expected to agree to and sign the db Primary Home-School Internet and Learning Platform User Agreement

Education

All children will receive planned E-safety lessons throughout Computing/PSHE (Personal Social and Health Education) lessons, these lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of assemblies to ensure all children are aware of the matter. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils 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. Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

Parents will be able to attend regular E-safety meetings, where they will also have the chance to ask questions regarding E-safety. They will also receive information via parents evenings and newsletters.

All staff will receive regular training regarding E-safety and an audit of their E-safety needs will be carried out. All new staff will receive E-safety training as part of the induction process, ensuring they are fully aware and understand the E-safety policy and the AUP. The E-safety Co-ordinator will be able to attend any regular updates provided by the Local Authority or other training schemes and report back to staff any new issues that they need to be aware of. The E-safety Co-ordinator will provide guidance for any member of staff that seeks it.

Filtering

Bishop William Ward receives a filtered broadband service through the broadband connectivity. This service is intended to stop users from accessing any material that would be regarded as inappropriate for the learning environment or illegal. If a virus is suspected on any school ICT equipment, use of the equipment must be stopped and the ICT (technical) Co-ordinator or ICT technician contacted immediately.

All staff and pupils will be made aware that there is also a monitoring system in place and any online activity can be traced.

Personal data

All personal data will be stored accordingly to the Personal Data Act 1998. Staff must use personal data on secure password protected machines and other devices, ensuring that they 'log off' at the end of any session. This will then minimise any chance of the data being seen by others. Devices must have virus and malware checking software.

| | Bishop William Ward Primary School

E-safety Policy |
|---|---|

Online learning

At Bishop William Ward we use db Primary and Purple Mash as our Learning Platforms. Through this, the children are able to communicate internally via the use of emails, blogs, forums and publishing work. These are monitored and tracked by teachers and Computing/ICT subject leaders. Misuse may result in the accounts being withdrawn. Only school email accounts will be used to communicate with children.

Each teacher will create their own 'communities' for the children to access. They will ensure content is appropriate. They will also have to approve work that the children wish to publish (internally).

If a pupil finds some inappropriate content on the learning platform, they can report it quickly and easily by clicking on the "Whistle" icon which can be found at the top, left hand corner of every page they visit. When a pupil clicks on the "Whistle" a dialogue box will appear which will allow them to enter more information, if required, but they can leave this section blank. This will be sent to the 'Whistle Monitors' who will investigate.

If a child is deemed to be using db Primary or Purple Mash inappropriately, their rights to the platform will be removed for an appropriate amount of time.

Emily Hale
Reviewed January 2018
Next review January 2019