BEDSTONE
www.bedstone.org

E-Safety Policy

at

Bedstone College

Author	DG
Date	1st September 2012/reviewed July 2014/reviewed August 2014/April 2015/August 2017/April 2018
Review Frequency	2 Yrs
Review Date	April 2020
Staff	HM
Gov	

WRITING AND REVIEWING THE e-SAFETY POLICY

The e-safety Policy is part the general college policy documentation and relates to various other policies including those for ICT, anti-bullying, sexting and for safeguarding.

This policy applies to all members of our college community, including boarders and those in our EYFS setting. Bedstone College is fully committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the college's Equality and Diversity Policy document.

The college will appoint an e-safety coordinator. In many cases this will be the Designated Person for Safeguarding as the roles overlap.

Our e-safety Policy has been written by the college, building on best practice and government guidance. It has been agreed by senior management and approved by governors

The e-safety Policy and its implementation will be reviewed annually

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The college has a duty to provide students with quality Internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students
- The college Internet access is provided by BT and the college systems include filtering appropriate to the age of students
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Students will be shown how to publish and present information appropriately to a wider audience.
- Students will be taught how to evaluate Internet content
- The college will seek to ensure that the use of Internet derived materials by staff and by students complies with copyright law
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Students will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector's World Safety Button.

Managing Internet Access

Information system security

- College ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority where appropriate

e-mail

- Students and staff may use web-based e-mail accounts on the college system
- Students must immediately tell a teacher if they receive an offensive e-mail
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Staff to student email communication must only take place via a college email address and will be monitored
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- The college will consider how e-mail from students to external bodies is presented and controlled
- The forwarding of chain letters is not permitted.

Published content and the college web site

- The contact details on the Web site should be the college address, e-mail and telephone number. Staff or students personal information will not be published
- The Headmaster or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing student's images and work

- Photographs that include students will be selected carefully. The college will look to seek to use group photographs rather than full-face photos of individual children. If full face photos are used on the Web site, they will never be accompanied by the full name of the child.
- Written permission from parents or carers will be obtained before photographs of students are published on the college Web site
- Parents should be clearly informed of the college policy on image taking and publishing, both on college and independent electronic repositories.

Social networking and personal publishing on the college learning platform

The college will control access to social networking sites, and consider how to educate students in their safe use e.g. use of passwords

Newsgroups will be blocked unless a specific use is approved

Students will be advised never to give out personal details of any kind which may identify them or their location

Students and parents will be advised that the use of social network spaces outside college brings a range of dangers for students of all ages

Students will be advised to use nicknames and avatars when using social networking sites

Students will be made aware of the dangers of accessing inappropriate material including material published by terrorist and/or extremist groups.

Managing filtering

- If staff or students come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Particular attention will be given to materials which might be seen as having the ability to radicalise young people (in accordance with the Prevent Strategy)

Managing videoconferencing (where the facility exists)

Students should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the students' age.

Managing emerging technologies

- Mobile phones and associated cameras will not be used during lessons. The use of the camera functionality in any such device during the college day is forbidden. The sending of abusive or inappropriate text messages is forbidden
- The use of games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering is forbidden
- Wherever possible staff will use a college phone where contact with students is required

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, and its replacement, GDPR (2018). See Separate polices and privacy notices for the GDPR.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT ' before using any college ICT resource
- The college will maintain a current record of all staff and students who are granted access to college ICT systems
- Parents will be asked to sign and return a consent form
- All students must apply for Internet access individually by agreeing to comply with the 'e-safety student code of conduct'
- Any person not directly employed by the college will be asked to sign an 'acceptable use of college ICT resources' before being allowed to access the Internet from the college site.

Assessing risks

The college will take all reasonable precautions to prevent access to inappropriate material. This includes offensive or illegal material and material connected to terrorist and/or extremist groups. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a college computer. The college cannot accept liability for the material accessed, or any consequences of Internet access.

The college will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headmaster
- Complaints of a safeguarding nature must be dealt with in accordance with college safeguarding procedures
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences for students misusing the Internet

Community use of the Internet

- All use of the college Internet connection by community and other organisations shall be in accordance with the college e-safety policy.

Communications Policy

Introducing the E-safety policy to students

- Appropriate elements of the e-safety policy will be shared with students
- e-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for students

Staff and the E-safety policy

- All staff will be given the College e-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers attention will be drawn to the College e-safety Policy in newsletters, the college brochure and on the college web site
- Parents and carers will from time to time be provided with additional information on e-safety
- The college will ask all new parents to sign the parent /student agreement when they register their child with the college.