

# INTERNET AND EMAIL

## 1. Policy Statement

*Bournemouth Collegiate School, along with the whole of the UCST group, recognises both the benefits and the threats of Internet use, but believes that the benefits greatly outweigh the disadvantages. Staff plan for and make use of ICT including Internet-based resources and e-mail to support their teaching. Effective access to employment increasingly requires computer and communications skills, and pupils need to develop these transferable skills at school. The value of Internet use at BCS is wide-ranging and includes.*

- *Providing access to information and educational resources for staff and students in support of the school's curriculum and extra-curricular activities - including participation in UCST and other on-line projects and networks*
- *Educational and cultural contact with pupils worldwide*
- *Supporting the training of pupils in the skills of critique and discrimination with respect to the quality, currency and relevance of on-line materials, and to help them develop rigorous approaches to the use and referencing of such materials*
- *Supporting the professional work and professional development of the school staff*
- *Supporting the school's information, promotion, marketing and business administration systems*

*BCS is committed to educating pupils, staff and parents on the safe use of the email and annual presentations are given to all, by the UCST ICT team.*

*BCS is fully committed to ensuring that the application of this Internet and Email document is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.*

*This document is applicable to all pupils in both senior and prep schools, including those in boarding and EYFS and BCS seeks to implement this policy through adherence to the procedures set out in the rest of this document.*

*In line with our Provision of Information policy, this document is available to all interested parties on our website and on request from the Senior school and Prep school offices and should be read in conjunction with the following documents: Child Protection, Anti-Bullying*

*This document is reviewed annually by the Senior Leadership Team, in consultation with the key personnel, or as events or legislation change requires. The next scheduled date for review is March 2012.*

## 2. Table of Contents

<b>1. Policy Statement</b>	<b>1</b>
<b>2. Table of Contents</b>	<b>2</b>
<b>3. Key Personnel</b>	<b>2</b>
<b>4. Procedures</b>	<b>2</b>
<b>A.Introduction</b>	<b>2</b>
<b>B.PROTECTING PUPILS ONLINE</b>	<b>3</b>
<b>C.EVALUATING AND MANAGING INTERNET CONTENT</b>	<b>3</b>
<b>D.USING THE INTERNET</b>	<b>4</b>
<b>E.EMAIL (ALSO RELEVANT TO TEXTS/ SOCIAL NETWORK SITE AND BLOGS)</b>	<b>5</b>

## 3. Key Personnel

Internet and Email in the Senior school is led by the Assistant Principal, Alison Davies

Internet and Email in the Prep school is led by the Head of Prep, Kay Smith

## 4. Procedures

### A. Introduction

Though much pupil use of the Internet is teacher-led, the Internet itself is largely devoid of barriers and will inevitably and rightly lead pupils to sites that were not selected by teachers. The BCS ICT system uses filters to block unsuitable sites, but despite taking all reasonable precautions to ensure that pupils only access suitable materials, the school cannot absolutely guarantee that unsuitable material will never be accessed. The responsibility for developing a mature and responsible approach to the Internet is shared with the pupils themselves and their families.

- The use of BCS computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990
- BCS recognises that use of the Internet, email systems and other ICT must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity.
- Tools to identify, assess and minimise risks are in place and are regularly reviewed
- Staff, parents, governors and advisers will work to ensure that every reasonable measure is being taken to ensure safe but effective use of the Internet and ICT
- These policies apply specifically to BCS technology on a BCS school site, but also apply in principal and with equal rigour to BCS use of mobile technology off-site (including PCs, laptops, webcams and digital video) and to mobile technology brought onto the BCS site (including laptops, mobile phones, personal digital assistants and portable media players)
- The Principal will ensure that the policy is implemented effectively

Sanctions are in place for deliberate access to inappropriate materials by staff, and in serious cases these include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

## **B. PROTECTING PUPILS ONLINE**

The internet is so fundamental to our learning and to our social and professional lives that we tend simply to take for granted its benefits and accept its flaws. So pervading is its reach, that we often downplay the possibility that it could be a threat - a serious threat - to our children. At BCS we acknowledge the power of the internet and seek every opportunity to exploit its many riches - but we also take seriously the fact that its use requires both discipline and discrimination.

Whether on a computer at school, a laptop at home, a games console or mobile phone, our pupils are increasingly accessing the internet and it cannot be assumed that they have the discipline or maturity to act with responsibility. Schools and families have a duty of care to ensure that young people are supported in developing good internet practice - and are protected when their internet behaviour falls below these standards.

On moral as well as legal grounds, we would all seek to protect young people from hidden threats in the real world, and take all reasonable steps to make sure that they are safe whatever they are doing. Online safety and responsibility skills are skills for life - they serve the school years but also lay the foundation for professional practice and for responsible citizenship. If a pupil understands and acknowledges the risks that they face online and can make sensible and informed choices, they will derive full benefit from the internet and stay safe whilst doing so – particularly from those people who might seek them out to harm them.

BCS therefore draws parents' attention to CEOPS (Child Exploitation Online Protection Service) which is dedicated to removing online risks of sexual abuse of children. They are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

The CEOPS approach is broad-based and pragmatic, drawing on the skills of police officers specialising in this area of criminality working with professionals from the wider child protection community and industry; seconded staff from organisations such as the NSPCC, teams sponsored by the likes of VISA and SERCO and experts from government and corporations such as Microsoft offering specialist advice and guidance. BCS suggests that parents visit [www.ceop.gov.uk](http://www.ceop.gov.uk) where they can access parent's resources to help them keep their child safe online and keep up-to-date on the implications of relevant technological changes.

## **C. EVALUATING AND MANAGING INTERNET CONTENT**

The key to safe and effective Internet use is the development of self-discipline supported by training in selecting relevant, rigorous and acceptable material. Staff and pupils are required to be responsible for the professionalism of their behaviour on-line just as they are anywhere else in the school.

- If staff or pupils accidentally access unsuitable sites, the URL (address) and content must be reported to a member of staff or the ICT manager - this avoids any supposition of deliberate misuse. The link to the site should be disconnected immediately the URL has been noted
- Staff, students and visitors are required not to seek to access offensive, abusive or discriminatory on-line materials deliberately
- Staff should ensure that pupils do not visit sites that require them to give personal details such as their name and place of residence unless these sites are fully certificated and known to the school.
- BCS requires that the use of Internet-derived materials by staff and pupils complies with copyright law
- Pupils are taught to critique the materials they read and are shown how to evaluate on-line information before accepting its accuracy.
- Pupils are taught to acknowledge (reference) the source of information when using Internet material in their own documents so as to avoid plagiarism (the school uses plagiarism identification software)
- Computers should only be used by pupils for school work and homework unless permission has been given (special arrangements apply to boarders)
- For both legal and computer security reasons, no programme files (executables) should be downloaded to a BCS computer (or uploaded from any memory device or medium)
- Any files brought to school from a home computer (including homework) or downloaded from the Internet should be virus scanned before being used on a BCS computer
- No pupil should send personal information (including name, address, email or telephone) from a BCS computer.

#### **D. USING THE INTERNET**

It is not possible or appropriate to constrain all aspects of acceptable and educationally-valuable Internet use (any more than this would be possible for books or libraries) but some general guidelines can be given:

- Teachers will guide students on the skills needed for on-line activities that will support the learning outcomes required by their curriculum
- Pupils will be trained how to make effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Pupils are encouraged to apply critical standards to all Internet-derived materials, specifically seeking to identify inaccurate or out-of-date material or hidden agendas and bias
- Staff and pupils should be aware that Internet use can be monitored and traced to the individual user. Discrete and professional conduct is essential.
- Staff and pupils are made aware of the measures they must take to protect against viruses, including checking removable media such as USB storage devices? Problems should be reported immediately to the ICT manager.
- Staff and pupils should immediately notify the ICT Manager if they have identified a possible security problem. They should not deliberately look for security problems because this could be interpreted as an illegal attempt to gain access.

While safe and responsible Internet access is the priority, BCS seeks to apply a balanced and proportionate approach that does not unduly limit the educational and professional value that staff and pupils can derive from web-based activities. It is emphasised that BCS takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. BCS cannot accept liability for the material accessed, or any consequences of Internet access.

Users should not regard their use of the Internet at BCS or the content of the materials they download or upload as confidential. They should not expect that email, voice mail or other information created or maintained in the system (even those marked “personal” or “confidential”) are strictly private, confidential, or secure. BCS does not monitor the use of the network, the contents of email, or the contents of voice mail messages as a routine matter other than through the use of automatic content filters. However, such monitoring may occur when required to protect the integrity of the system or to comply with legal obligations. The School reserves the right to inspect the contents of uploaded materials, email or voice mail messages in the course of an investigation of inappropriate behaviour by pupils or staff.

#### **E. EMAIL (ALSO RELEVANT TO TEXTS/ SOCIAL NETWORK SITE AND BLOGS)**

Staff and pupils need to be aware that emails are easily forwarded so it is imperative that they should be professional and meet all the standards of content and presentation that you would expect with a letter on school headed notepaper. Make the assumption that emails will become public, and avoid writing anything that you or the school would regret. None of the following should be deliberately sent:

- Pornographic language or pictures
- Information which may be considered offensive or threatening to others
- Defamatory or illegal information
- Copyright material as an attachment

Email is an extremely effective mode of communication, but it can (if allowed) become a tyranny. Consider the following guidelines for your use of email:

- Schedule answering emails into the school day, but do not allow this process to take automatic priority over other school activities.
- The immediacy of email is an opportunity rather than an obligation. If an instant response is possible, then this may be the most effective way of handling the communication - but be prepared to allow time for proper reflection and information gathering. Acknowledge the email and offer a considered response within 7 days, then flag the email so that it is not forgotten.
- Remember that the most appropriate response to an email may be a phone call or meeting.
- Copy people into an email only if this is to their benefit. There is a fine balance between keeping staff informed (a very important function) and overwhelming them with spurious communications.
- Avoid getting hooked into iterative email debates with one pupil or set of parents to the detriment of others. Seek SLT advice or intervention if this seems likely.

- In many cases, sensitive information should be sent by mail rather than email.
- Under no circumstances should staff leave their mailbox open and unattended.
- The BCS system can and does monitor e-mail. The content-checking filters are revised and added to on a regular basis. E-mails sent from the school which contain proscribed phrases or key words are blocked and referred for approval. This is both a security and safety measure.

The following uses of email should be regarded as unacceptable or inadvisable (particularly for pupils):

- Revealing personal details such as name, address or contact details to people who are not known to you
- Revealing your password to anyone else, or using someone else's password
- Sending or distributing "chain letters", no-matter how good the cause appears to be
- Using obscene, threatening, defamatory, discriminating or harassing language. BCS takes verbal bullying very seriously.
- Using the BCS email system for commercial or political purposes

Staff and pupils should be extremely cautious when using email to communicate confidential or sensitive content, and should not assume that email is private and confidential. It is especially important that users are careful to send messages only to the intended recipient(s). Particular care should be taken when using the "Reply" or "Reply all" commands. Staff and pupils must accept that there is no guarantee of privacy within the BCS ICT system. They should not assume that email, voice mail, or other information (even those marked "personal" or "confidential") are in fact strictly private, confidential or secure.