BOURNEMOUTH SCHOOL FOR GIRLS – SCHOOL POLICY STATEMENT

E-SAFETY

23

CONTENTS

INTRODUCTION AND POLICY STATEMENT

Aims of Policy

- To raise the awareness of all school staff of the importance of e-safety and of their responsibilities.
- To ensure pupils and parents are aware of the importance of e-safety.
- To ensure that both staff and pupils/students are protected from both accidental and malicious misuse of ICT.

Responsibilities

The school will:

- appoint a lead governor responsible for e-safety within the school (who will ordinarily be the governor responsibility for Safeguarding and Child Protection)
- appoint a designated e-safety officer who is a member of the Senior Leadership Team (David Sims). A deputy will also be appointed (Ms A Collins)
- require teachers, staff and volunteers to implement the e-safety procedures, school policy and good practice guidelines
- ensure that staff have undertaken e-safety training.

Designated e-safety Person will:

- circulate the e-safety Policy to all staff and governors
- provide the school's e-safety policy to any parent upon request and publish it on the website
- ensure that all new staff including supply teachers receive e-safety induction
- ensure whole school e-safety training every 3 years (as part of Safeguarding training)
- act as a point of reference for e-safety concerns
- take responsibility for collating and securely storing records of incidents and concerns.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils/students 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/students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils/students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information.
- Pupils/students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education – pupils/students

E-Safety education will be provided in the following ways:

- a planned e-safety programme is provided as part of ICT/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- rules for use of ICT systems/internet will be posted in all ICT rooms.

Use of digital and video images - photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils/students, instant use of images that they have recorded themselves or downloaded from the internet.

However, staff and pupils/students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils/students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils/students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils/students will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils/students full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils/students are published on the school website.
- Pupils/students work can only be published externally with the permission of the pupils/students and parents or carers.

PUPIL / STUDENT ACCEPTABLE USE POLICY

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

ICT ACCEPTABLE USE POLICY FOR PUPILS

I understand that I must use school ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password with secrecy – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource:

- I understand that the school ICT systems (including e-mail) are intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for playing games, file sharing, or video broadcasting, e.g. You Tube.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other users' files without the owners' knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will not take or distribute images, e.g. photos or videos of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held/external devices (e.g. mobile phones) in school if I have permission and never in an IT Suite. I understand that if I do use my own devices (e.g. USB devices) in school I will follow the rules set out in this agreement in the same way as if I were using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails unless I know and trust the person/organisation that sent the email, because of the risk of the attachments containing viruses or other harmful programs.
- I will not install or attempt to install programs of any type on a machine or store programs on a computer, nor will I try to alter computer settings.
- I will not attempt to use web based e-mail, chat and social networking sites in school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright I will not try to download copies including music and videos.
- When I am using the internet to find information I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, covered in this agreement, when I am in school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of school in a way that is related to my being a member of this school, e.g. communicating with other members of the school, accessing school email, VLE, websites etc.

Name of Pupil			
Form:			
Signed		Date	

RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that may be made to any apparent or actual incidents of misuse:

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of House / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓			✓
Unauthorised use of non-educational sites during lessons	✓				✓			✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓			✓			✓
Unauthorised use of social networking / instant messaging / personal email	✓	✓	✓	✓		✓			✓
Unauthorised downloading or uploading of files					✓	✓	✓		
Allowing others to access school network by sharing username and passwords					✓	✓	✓		
Attempting to access or accessing the school network, using another student's / pupil's account					✓	✓	✓		
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓						✓
Corrupting or destroying the data of other users		✓			✓		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓		✓			✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓						✓
Using proxy sites or other means to subvert the school's filtering system			✓		✓	✓	✓		✓
Deliberately accessing or trying to access offensive or pornographic material			✓	✓	✓	✓	✓		✓

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff and other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons for calls/texts				✓				✓
Use of mobile phones for other functions, e.g. internet	✓						✓	
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones or other camera devices		✓					✓	
Use of hand held devices e.g. PDA's, PSP's	✓				✓			
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails	✓				✓			
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓				✓			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to David Sims (staff users) or to a teacher (student users) – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Any digital communication between staff and students / pupils or parents / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

PUPIL/STAFF COMMUNICATION PROTOCOL

Context

In the light of the explosion in communication technologies and as a result the ease of access to data of many forms and types it is important that staff are not put in a position whereby they, the school or pupils can be comprised in any way. As a result it is important that communication between pupils and adults, by whatever method should take place within clear and explicit professional boundaries. Adults should be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

General

- All portable or other computers brought on-site or attached to the Bournemouth School for Girls network remotely must be covered by anti-virus software. Anti-virus software must be kept up to date and operational.
- Staff must not copy software illegally. All copyright restrictions must be observed. Staff must not bring portable or other computers on site that have illegal software loaded onto them.
- Staff must not load or modify software on the Boumemouth School for Girls computers without authorisation from the Network Manager. Staff must not copy data or software from the network without proper authorisation.
- Staff must not use the Boumemouth School for Girls computers for unauthorised purposes.
- Each staff member is allocated a work area on the network, which must be protected by them using their own password. This password is to remain confidential and should be changed on a regular basis.
- Staff must not knowingly access, or attempt to access another individual's data or information without proper authorisation.
- Although every care will be taken to ensure adequate backing up of data held on the Boumemouth School for Girls network, Boumemouth School for Girls cannot accept responsibility for loss of data and software.
- It is the responsibility of staff using portables to arrange their own backing up of data and software. It may be appropriate to backup data only on a weekly basis to your individual network area. Advice can be sought from the Head of ICT or the Network Manager.

This means adults should:

1. Carefully review all Internet sites where you have recorded any personal information that could be accessed by students, parents or employers. Do not post information/photographs about yourself publicly that could be potentially damaging to your career or could bring the school into disrepute or breach the integrity of the ethos of the school if seen by employers, pupils, parents or colleagues. Ensure that privacy levels on social networking sites are set to protect yourself as fully as possible i.e. do not accept 'friends of friends'. Do not add current pupils to contact lists. Relationships with ex-pupils can cause a problem with the potential suggestion that contact was made before the student left.
2. Not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites.
3. Only use equipment e.g. mobile phones, provided by the organisation to communicate with children.
4. Only make contact with children for professional reasons and in accordance with any organisation policy.

5. Recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible.

6. Not use internet or web-based communication channels, other than the school's Virtual learning Environment and email server to send messages to students/pupils.

7. Ensure that if a social networking site is used, details are not shared with students/pupils and privacy settings are set at maximum.

8. Ensure that they do NOT give their personal contact details to children and young people including personal e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

E-mail or text communications between an adult and a child or young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Unsuitable / Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other ICT systems. Other activities e.g. Cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images.
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation.
- Adult material that potentially breaches the Obscene Publications Act in the UK.
- Criminally racist material in UK.
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

The following activities are prohibited:

- Using school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGFL and/or the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords.)
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gaming (non educational).
- File sharing of copyrighted material.
- Use of social networking sites.

Appendix 1

Links to other organisations or documents

SOUTH WEST GRID FOR LEARNING:
"SWGfL Safe" - http://www.swgfl.org.uk/safety/default.asp

Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.gov.uk/

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World")
http://www.dcsf.gov.uk/byronreview/

Becta
Website e-safety section - http://schools.becta.org.uk/index.php?section=is

Developing whole school policies to support effective practice:
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835

"Safeguarding Children in a Digital World"
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

NATIONAL EDUCATION NETWORK
NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

CYBER-BULLYING
DCSF - Cyberbullying guidance
http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007

Teachernet
http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Teachernet "Safe to Learn – embedding anti-bullying work in schools"
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/

East Sussex Council – Cyberbullying - A Guide for Schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

References to other relevant anti-bullying organisations can be found in the appendix to the DfE publication "Safe to Learn" (see above)

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance -
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Digizen – "Young People and Social Networking Services":
http://www.digizen.org.uk/socialnetworking/

Ofcom Report:
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

MOBILE TECHNOLOGIES
"How mobile phones help learning in secondary schools":
http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02_a&rid=15482

Mobile phones and cameras:
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

DATA PROTECTION AND INFORMATION HANDLING
Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

BECTA - Data Protection:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

To be read in conjunction with the Communication Policy and Email Protocol.

Reviewed July 2016
Next review July 2017