British School of Gran Canaria

E-Safety and use of Technologies

Policy Document

Contents

THE BRITISH SCHOOL OF GRAN CANARIA

E-SAFETY AND USE OF TECHNOLOGIES POLICY

1. Definitions

Throughout this document the following words, terms and phrases have the following meanings:

BSGC – British School of Gran Canaria, also referred to as the School.

Pupils – include the term children and students.

School – includes both the Tafira and South School sites.

School community – includes all pupils and employees.

Senior teacher – member of the SMT.

E-Safety Coordinator – the Computer Science teacher in the secondary school.

Staff includes all employees of the school, i.e. teachers, administrators, canteen workers and ancillary personnel.

SMT – Senior Management Team.

Network Manager – Senior IT Technician employed by the school

Data Manager – Contracted manager, currently Prodat.

Hand-held device – Mobile phone, tablet, smart watch or other personal device that can be connected to the Internet. Also included: digital cameras, both stand-alone and integrated into another personal device.

2. Context

New technologies have become integral in the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

This e-Safety Policy explains how BSGC intends to help young people (and their parents / carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

3. Rationale

The purpose of this policy is to:

a. set out the conduct expected of all members of the School community with respect to the use of ICT-based technologies;
b. safeguard and protect the pupils and staff of BSGC;
c. assist school staff to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice;
d. set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use;
e. have clear procedures to deal with online abuse such as cyberbullying which are cross referenced with other school policies;
f. ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action shall be taken;
g. minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

4. The Risks

The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

Content

- exposure to inappropriate content, including online pornography;
- ignoring age ratings in games;
- substance abuse;
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- hate sites.

Contact

- grooming;
- cyber-bullying;
- identity theft and password security.

Conduct

- illegal downloading;
- privacy issues;
- digital footprint and online reputation;
- health and well-being issues through overuse;
- sending and receiving of personally intimate images (sexting);
- copyright and plagiarism;
- excessive use which may impact social and emotional development.

5. Scope

This e-Safety policy is referenced in other school policies: Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

This policy applies to all members of the BSGC community including visitors and community users who have access to and are users of school ICT systems, both in and out of school.

The school reserves the right to impose sanctions on school community members whose unacceptable use of ICT outside of school affects well-being of the BSGC community. Appendix A provides a matrix of identified inappropriate activities.

6. Roles and Responsibilities

The key staff involved in monitoring and reviewing this policy are:

- E-Safety coordinator
- Network manager
- E-Safety Governor

Other key roles are:

- Head
- SMT
- Technical Support Staff

A detailed clarification of roles is set out in Appendix B.

7. Policy Statements

Details of how BSGC manage the ICT and Infrastructure are given in section 9 and at Appendix C.

7.1 Education – pupils

- A planned e-Safety programme is provided as part of ICT, PHSE and other lessons being regularly revisited to cover use of ICT and new technologies in and beyond school – Appendix D for Pupil ICT Use Matrix.
- Key e-Safety messages are reinforced and regularly conveyed in assemblies, tutorial and pastoral activities.
- Pupils are taught to be critically aware of the materials and content accessed on-line and to validate the accuracy of information.
- Pupils are helped to understand the need for the pupil's Acceptable Use Policy (Appendix E) and encouraged to adopt safe and responsible use, both within and outside school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff should act as good role models in their use of ICT and the Internet. A Staff Permitted Communications Grid is presented in Appendix F.

7.2. Education & Training – Staff & Governors

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policies (Appendix G).
- This e-Safety policy will be presented to and discussed by staff in meetings and INSET days ensures that staff and pupils understand the issues associated with commercial use of the Internet, including pop-ups; buying on-line; on-line gaming / gambling and how to report misuse or access to inappropriate materials.

7.3. Parent Awareness and Training

Through this Policy the School will raise the awareness of e-Safety issues with parents by the implementation of the Acceptable Use Agreements.

8. Expected Conduct and Incident Management

8.1. Expected Conduct

The School Community is required to:

- use the school ICT systems in accordance with the Acceptable Use Policy;
- understand the importance of adopting good e-Safety practice at all times;
- acknowledge and understand the consequences of misuse or access to inappropriate materials;
- recognise and report instances of information abuse, misuse or access of inappropriate materials;
- acknowledge and adhere to the policy on the use of Hand-held Devices and understand how these policies relate to taking / use of images and cyber-bullying;

In addition, staff are required to read the school's e-Safety policy and comply with expectations related to the private use of school ICT systems, Hand-held devices and understand Data Protection. See Appendix H.

Pupils shall have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers shall be aware that their children shall use the Internet, as well as other technologies in school and shall know and understand what the 'rules of appropriate use' are and what sanctions result from their misuse.

8.2. Incident Management

At this School:

- there is strict monitoring and application of the e-Safety policy and a differentiated and appropriate range of sanctions;
- all members of the community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed in dealing with e- Safety issues e.g. http://www.protegeles.com and https://www.is4k.es/necesitas-saber/ciberacoso-escolar, Spanish websites providing advice for pupils, teachers and parents;
- there is a continuous cycle of enhancement to the policy to keep up with technology advances, and monitoring and reporting of e-Safety incidents to the SMT and Governors;
- parents/carers of those involved are specifically informed of e-Safety incidents involving young people for whom they are responsible;
- the Head shall contact the Police if one of our staff or pupils receives or sends online communication that we consider is particularly disturbing or breaks the law.

8.3. Handling complaints

The school shall take all reasonable precautions to ensure e-Safety. As it is not possible to guarantee that unsuitable material can never appear on a school computer or Hand-held device, the school cannot accept liability for material accessed, or any consequences of Internet access.

- The School Community is given information about unacceptable use and possible sanctions which may include:
  - interview/counselling by tutor /Senior Teacher - Pastoral Care/ Head of Primary / Head;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which shall ultimately prevent access to files held on the system, including examination coursework];
  - referral to Police.
- The E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Director directly.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

9. Managing the ICT Infrastructure

9.1. Internet access, security, virus protection and filtering

This school manages the ICT infrastructure by applying a variety of safeguards. This is the responsibility of the Network manager and E-Safety Coordinator to keep up to date and current.

9.2. Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

9.3. E-mail

The school;

- provides staff with an email account for their professional use and makes clear personal email shall always be through a separate account;
- reserves the right to contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- shall ensure that email accounts are maintained and up-to-date;
- raises awareness that spam, phishing, malware, ransomware and virus attachments can make e-mails dangerous and damage not just one email account but the school's entire ICT system.

Pupils;

- are introduced to, and use e-mail as part of the ICT scheme of work;
- are allocated a school e-mail account and personal password that they must manage within the school e-safety guidelines;
- are taught about the safety and 'netiquette' of using e-mail both in school and at home;

9.4. School website

- The Head takes overall responsibility to ensure that the website content is accurate and presentation quality is maintained, while delegating day-to-day responsibility to the school's website coordinator.
- Most material is the school's own work but where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The points of contact on the web site are the school address, telephone number and email address. Home information or individual e-mail identities are not published.
- Photographs published on the website do not have full names attached and have relevant parental permissions archived.

9.5. Social networking

- Networking for school purposes can be extremely useful but permission must be given by the school before starting. All interaction must be public, and the forum must only be used for school reasons.

10. Equipment and Digital Content

10.1 Staff use of personal Hand-held devices

- Personally owned Hand-held devices brought into school are entirely at the individual's own risk with respect to damage or loss and must be switched off or silent at all times.
- The School reserves the right to search the content of any Hand-held devices on the school premises where there is a reasonable suspicion that it shall contain undesirable material, including those which promote pornography, violence or bullying.
- Staff must not use their personally owned Hand-held devices during lesson times.
- Staff shall be issued with a school phone where contact with pupils, parents or carers is

required. There shall be extenuating circumstances for example when engaged on residential trips or when a member of staff has private classes with a pupil.

- Hand-held devices may be used to stream music or videos required by pupils or teachers for educational purposes but always under the strict supervision of a member of staff.

10.2 Pupils' Use of Personally Owned Hand-held Devices

- The School strongly advises pupils not to bring Hand-held devices into school. If Primary pupils need to bring them to school for any reason, they shall be handed to the class teacher for safe keeping until the end of the school day.
- If for good reason a pupil needs to contact their parents or carers, they shall be allowed to use a school phone. Parents must not contact their child via their Hand-held device during the school day, but via the school office.
- If a pupil breaches the school policy, then the Hand-held device shall be confiscated and held in a secure place in the school office. Hand-held devices shall be released to pupils, parents or carers at an appropriate time decided by the Head of Sector.
- Student can use Hand-held devices for educational purposes only under the explicit instruction of a member of staff whose has previously sought approval from a senior manager.

10.3 Digital images and video

- Parental / carer permission is sought for digital photographs or video involving their pupil as part of the school agreement when their child joins the school.
- The identification of pupils in online photographic materials or the inclusion of the full names of pupils in the credits of any published school-produced video materials / DVDs is prohibited.
- Access to social networking sites is blocked unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-Safety education programme as part of their Computing scheme of work.
- Pupils are taught about the risks of posting personal photographs on-line.
- Pupils are taught that they must not post images or videos of others without their permission, and the risks of doing so.

BSGC requests that parents support the school's e-Safety policy by ensuring the safe and appropriate use of technology and the Internet at home

Appendix A – Inappropriate Activities Grid

Unsuitable / inappropriate activities

Some Internet activity, e.g., accessing pupil abuse images or distributing racist material is illegal and is banned from school and all other ICT systems. Other activities including Cyber-bullying is not tolerated and may lead to a school sanction and possible criminal prosecution. There are, however, other activities which although legal are inappropriate in a school context, either because of the age (see Appendix I) 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 that the users, as defined below, shall 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:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Pupil sexual abuse images					√
Promotion or conduct of illegal acts, e.g. under the pupil protection, obscenity, computer misuse and fraud legislation					√
Adult material that potentially breaches the Obscene Publications Act in the UK and Spain					√
Criminally racist material in the UK and Spain					√
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 shall be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				√	
Using school systems to run a private business				√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by 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				√	
Creating or propagating computer viruses or other harmful files				√	
Carrying out sustained or instantaneous high-volume network traffic that causes network congestion and hinders others in their use of the internet. (Denial of service attack.)				√	
On-line gaming (educational)		√			
On-line gaming (non- educational)				√	
On-line gambling				√	
On-line shopping / commerce			√		
File sharing			√		

Use of social networking sites			√		
Downloading video broadcasting (YouTube)	√				
Uploading to video broadcast (YouTube)			√		

Appendix B – E-Safety Roles and Responsibilities

Role	Key Responsibilities
Head	• takes overall responsibility for e-Safety provision • takes overall responsibility for data and data security • ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements • responsible for ensuring that staff receive suitable training to carry out their e-Safety roles and training other colleagues, as relevant • aware of procedures to be followed in the event of a serious e-Safety incident • receives regular monitoring reports from the E-Safety Co- ordinator • ensures that there is a system in place to monitor and support staff who carry out internal e-Safety procedures (e.g. network manager)
E-Safety Co-ordinator / Computing Curriculum Leader	• takes responsibility for e-Safety and has a leading role in establishing and reviewing the school e-Safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-Safety education is embedded across the curriculum • liaises with school ICT technical staff to ensure secure management of the ICT infrastructure • communicates regularly with SMT and the designated e-Safety Governor to discuss current issues, review incident logs and filtering logs • ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • ensures that an e-Safety incident log is kept up to date • facilitates training and advice for all staff • oversees the delivery of the e-Safety element of the Computing curriculum • is regularly updated in e-Safety issues and legislation
Governors	• ensure that the school follows all current e-Safety advice to keep the pupils and staff safe • appoint an e-Safety Governor to monitor this aspect of the school and update Governors on important issues • ensure the school e-Safety Policy is reviewed for effectiveness and approved by Board of Governors • support the school in encouraging parents and the wider community to become engaged in e-Safety activities

Role	Key Responsibilities
Network Manager and Data Manager	• reports any e-Safety related issues that arise to the e-Safety coordinator • ensures that users shall only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • ensures the security of the school ICT system • ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • ensures the school's policy on web filtering is applied and updated on a regular basis • keeps up to date with the school's e-Safety policy and technical information to effectively carry out their e-Safety role and to inform and update others as relevant • ensures that the use of the network, Virtual Learning Environment (Moodle), remote access and email are regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator for investigation, action or sanction • ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
Teachers	• embed e-Safety issues in all aspects of the curriculum and other school activities • supervise and guide pupils carefully when engaged in learning activities involving online technology • ensure that pupils are fully aware of research skills and of legal issues relating to electronic content such as copyright laws • act as role models in their work and behaviour in personally upholding and promoting the expectations set out in the BSGC e- Safety policy
All staff	• must read, understand and help promote the school's e-Safety policies and guidance • must read, understand, sign and adhere to the school staff Acceptable Use Agreement • report any suspected misuse or problem to the e-Safety coordinator • maintain an awareness of current e-Safety issues and guidance e.g. through CPD • model safe, responsible and professional behaviours in their own use of technology

Role	Key Responsibilities
Pupils	• must read, understand, sign and adhere to the Pupil Acceptable Use Agreement (NB: at KS1 & KS2 it would be expected that parents / carers would sign on behalf or alongside the pupils' signatures)
Parents/carers	• to support the school in promoting e-Safety and endorse the Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to consult with the school if they have any concerns about their children's
External groups	• any external individual / organisation shall sign an Acceptable Use Agreement prior to using any equipment or the Internet within school

Appendix C – Management of ICT Infrastructure

This school:

- has educational, filtered, secure broadband connectivity to the Internet;
- ensures network health through use of an anti-virus software;
- blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- blocks pupil access to music download or shopping sites – except those approved for educational purposes;
- is vigilant in its supervision of pupils' ICT use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- requires staff to preview websites before use and encourages use of the school's Learning Platform as a key way to direct pupils to age and subject appropriate web sites;
- is vigilant when conducting image searches with pupils, e.g., Google image search;
- informs all users that Internet use is monitored;
- informs staff and pupils that that they must report any failure of the filtering systems directly to the system manager;
- makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes;
- provides advice and information on reporting offensive materials, abuse/ bullying etc. to pupils, staff and parents;
- reserves the right to refer any material we suspect is illegal to the appropriate authorities, e.g., the Police.

Appendix D – Pupil ICT Use Grid

Incident involving pupils	**Teacher to use school behaviour policy to deal with**	**Refer to Head of School**	**Right to refer to police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that shall be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		√	√	√
Unauthorised use of non-educational sites during lessons	√			√
Unauthorised use of Hand-held 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 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		√		√
Continued infringements of the above, following previous warnings or sanctions		√	Police referral	√
Actions which shall 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		√		√
Accidentally accessing offensive or pornographic material and failing to report the incident		√		√

The guidance in this policy shall be implemented with cross reference to the School's Pupil Protection, Anti-Bullying and Behaviour Policies. Note: attempts have been made to synchronise guidance and sanctions.

Appendix E – Pupil Acceptable Use Agreement

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use shall result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I shall only access the school network through my authorised username and password when issued to me in Secondary School. I shall not use the passwords of others.
- I shall not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file-sharing or video broadcasting.
- I shall not try to upload, download or access any materials which are illegal, inappropriate or which shall cause harm and distress to others.
- I shall not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I shall not try to install programmes on any school computer or try to alter computer settings.
- I shall only use my personal Hand-held devices (e.g., mobile phone, iPod, smart watch, digital camera) in school at times that are permitted. This also applies to commuting to and from school on a school bus, or to contacting parents after participation in an extra- curricular activity. When using my own Hand-held devices, I understand that I must follow the rules set out in this document.
- I shall carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I shall not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I shall not disclose personal information about myself or others when on-line. I shall not arrange to meet 'on-line friends' unless supervised by an adult.
- I shall not take or distribute images of anyone without their permission.
- I shall report to a teacher any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I shall not try to download copies, including music and video. I shall only use the work of others found on the Internet in my own work with their permission.
- I shall take care to check that information I find on the Internet is accurate and understand that some content found on the Internet can be untruthful or misleading.

- I shall immediately report any damage or faults involving IT equipment, however this shall have happened.

Name of Pupil ……

Signed ……..

Date …….

Appendix F - Permitted Communications Grid

Communications

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

	Staff and other adults					**Pupils and young people**			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones brought to school	√					√			
Mobile phones used in lessons		√						√	
Use of mobile phones in social time	√							√	
Taking photographs on Hand-held devices		√						√	
Use of school email for personal emails				√					√
Social use of chat rooms				√					√
Use of social network sites				√				√	
Use of educational blogs	√					√			

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

- The official school email service shall be regarded as safe and secure and is monitored. Staff and pupils shall therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person, in accordance with 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 pupils or parents/carers (email, chat, Learning Platform, etc.) must be professional in tone and content. These communications shall 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.
- Pupils shall be taught about email safety issues, such as the risks attached to the use of personal details. They shall also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information shall not be posted on the school website and only official email addresses shall be used to identify members of staff.

Appendix G – Staff Acceptable Use Agreement

Responsible Use Agreement

I commit to using BSGC 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. I recognise the value of the use of ICT for enhancing learning and will seek opportunities for my learners to access opportunities to gain from the use of ICT. I shall, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with pupils.

For my professional and personal safety:

- I understand that the school may monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, Learning Platform, etc.) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I shall only use systems for personal or recreational use within the policies and rules set down by the school.
- I shall not disclose my username and password to anyone else, nor shall I try to use any other person's username and password.
- I shall immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person (see policy flowcharts).

I shall be professional in my communications and actions when using school ICT systems or personal technologies whilst in school:

- I shall not access, copy, remove or otherwise alter any other user's files without their express permission.
- I shall communicate with others in a professional manner. I shall not use aggressive or inappropriate language and I appreciate that others shall have different opinions.
- I shall ensure that when I take and/or publish images of others I shall do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I shall use chat and social networking sites in accordance with the school's policies (Child Protection / Safeguarding Policy and Rule 6e of this document).
- I shall only communicate with pupil and parents/carers using official school systems. Any such communication shall be professional in tone and manner.
- I shall not engage in any on-line activity that would compromise my professional responsibilities.

BSGC has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use any personal Hand-held device in school, I will use as if I were using school equipment.
- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (pupil sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or shall cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless allowed by school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or learner data to which I have access, shall be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I shall immediately report any damage or faults involving equipment or software, however this shall have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of BSGC ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment at BSGC.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and, in the event of illegal activities, the involvement of the police.

I understand and agree to the guidelines set out above.

Name ……..

Signed …….

Date ……...

Appendix H - Staff ICT Use Grid

Incidents involving members of staff	Refer to the Director *See below	Refer to technical support staff for action re filtering, security etc.	Referral to Statutory Authority Potential Disciplinary Action
Deliberately accessing or trying to access material that shall be considered illegal (see list in earlier section on unsuitable or inappropriate activities).	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√		√
Excessive or inappropriate personal use of the Internet/social networking sites/ instant messaging/ personal email	√	√	√
Unauthorised downloading or uploading of files	√	√	√
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	√	√	√
Careless use of personal data e.g. holding or transferring data in an insecure manner	√		√
Deliberate actions to breach data protection or network security rules	√	√	√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with pupils/ pupils	√	√	√
Actions which shall compromise the staff member's professional standing	√		√
Actions which shall 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	√	√	√
Breaching copyright or licensing regulations	√	√	√
Continued infringements of the above, following previous warnings or sanctions	√		√

*In event of breaches of policy by the Director, refer to the Chair of Governors.

Appendix I – Age Appropriate Computing Curriculum Notes

- STOP and THINK before you CLICK!
- to develop a range of strategies to evaluate and verify information before accepting its accuracy
- to be aware that the author of a web site / page shall have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- to understand how search engines work and to understand that it affects the results seen at the top of the listings
- to understand acceptable behaviour when using an online environment or email, i.e., be polite, no bad or abusive language or other inappropriate behaviour; keep personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they shall be careful in online environments
- to understand why young people should never post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have enabled privacy settings
- to understand why people must not post pictures or videos of others without their permission
- to know not to download any files – such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- to understand why and how some people 'groom' young people for sexual reasons
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, e.g., a parent or teacher.