S103/A0621

BANSTEAD

COMMUNITY JUNIOR

SCHOOL

COMPUTING AND ON-LINE SAFETY POLICY

2020

School Resources Committee

Prepared by:	Carley Knight/R Holyoake
Created/reviewed:	June 2020
Date of next review:	June 2021

CONTENTS

BANSTEAD COMMUNITY JUNIOR SCHOOL

COMPUTING AND ON-LINE SAFETY POLICY

1. Teaching and Learning

1.1 Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school 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 pupils.

1.2 Internet use will enhance learning

- The school Internet access is provided by Connectus and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. by minimizing the screen, talk to a responsible adult, using the CEOP Report Abuse icon or Hector Protector.

2. Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Staff access to school networks will be controlled by **personal** passwords which are changed regularly.

- The security of school IT systems will be reviewed regularly.

- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.

- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.
- Security strategies will be discussed with the Surrey On-line Safety Team.

2.2 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published apart from names (generally first name).
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will be avoided on the Website as appropriate, particularly in association with photographs, unless special permission has been given by parents/carers.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Parents should be clearly informed of the school policy on image taking and publishing.

2.4 Use of Social media

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- The school's Facebook and Twitter feed will be managed by staff authorized to do so by the Senior Management Team only.
- Staff and pupils should use caution to ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Internet safety is taught as part of the curriculum.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.5 Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Internet Safety Co-ordinator/Network Manager.
- Senior staff/Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.6 Use of personal devices

- Personal equipment may be used by staff to access the internet, provided their use complies with the on-line safety policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used on school premises or for school business.

2.7 Use of Cloud-based services

The school utilises Cloud-based Services, for backup, Pupil Assessment, communication and payment systems.

It is the school's responsibility (together with the services of the cloud based provider) to ensure the security of the data by ensuring:

- Where the data is backed up and how often it is backed up? Note the legal requirements for data to remain hosted within the EU or in a country that is Internationally designated a data Safe Harbour
- What is the data recovery process and how is the data encrypted in transit across the internet?
- How the data is protecting pupils and staff privacy? And how does the service provider ensure that the information is secure?
- Who owns the data stored in the cloud and who has access to it?

It is essential to check that the service provider doesn't share contact details with third party companies and also to investigate the reliability of the system.

Parental permission will be sought if the school decides to utilise other cloud based services inc. Google Apps and Microsoft 365 before student accounts are created.

2.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

2.9 E-mail

- Pupils must immediately tell a teacher if they receive offensive e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- **Pupils and staff may only use approved e-mail accounts on the school IT systems.**

- Staff to pupil or families e-mail communication must only take place via a school email.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known and the email is expected.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

3. Policy Decisions

3.1 Authorising Internet access

- All staff must read and sign the ‘Acceptable Use Policy/Computing Code of Conduct before using any school computing resource.
- The school will maintain a current record of all staff and pupils who are granted access to school computing systems/Internet.
- **Access to the Internet by pupils will be with adult supervision.**
- Parents will be asked to sign and return a consent form.

3.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Connectus can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit computing use to establish if the Computing and On-line Safety Policy is adequate and that the implementation of the policy is appropriate and effective.

3.3 Handling On-line 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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

4. Communications Policy

4.1 Introducing the Computing and On-line Safety Policy to pupils

- Appropriate elements of the Computing and On-line Safety Policy will be shared with pupils
- On-line Safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of On-line Safety issues and how best to deal with them will be provided for pupils

4.2 Staff, volunteers and the Computing and On-line Safety Policy

- All staff will be given the School's Computing and On-line 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 computing use will be supervised by senior management and have clear procedures for reporting issues.

4.3 Enlisting parents' support

- Parents' and carers' attention will be drawn to the School's Computing and On-line Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on On-line Safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

5. Failure to Comply

- Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.

Spiritual, Moral, Social and Cultural Development

Where possible, lessons, either through specific planning or ad-hoc opportunities, will promote the spiritual, moral, social and cultural development of pupils and their understanding of the role of society and their place within it. Through this approach, the school and specific subject teaching, aims to prepare pupils for the opportunities, responsibilities, experiences and challenges of their current and later lives.

British Values

The School will ensure in policy and practice that it adheres to the fundamental British Values as detailed in Ofsted Handbook for Inspection, August 2016.

The fundamental British Values include valuing democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs. The pupils will be taught to develop and demonstrate skills and attitudes that will allow them to participate fully in and contribute positively to life in modern Britain.

Changes highlighted in yellow.

Appendix 1 Pupil Acceptable Use Agreement / On-line Safety Rules

Dear Parent/Carer

Computing including the internet, email, laptops, digital cameras etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any computing.

Please discuss these On-line Safety rules with your child. If you have any concerns please refer to the school website (www.bcjs.org.uk) where there are links to other helpful sites with a wealth of information on this subject.

- I will only use computing in school for school purposes.
- I will make sure that all computing contacts with other children and adults are responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will minimise my screen or close the lid and tell my teacher immediately.
- I will not send to children or adults anything that could be considered unpleasant or nasty.
- *I will not give out personal details such as my phone number or home address.*
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using computing because I know that these rules are to keep me safe.
- I know that my use of computing can be checked and that my parent/carer contacted if a member of school staff is concerned about my On-line Safety.
- I understand if there is a concern about internet misuse I will speak to the Headteacher.

………………………………………………………………………………………………….

Parent/Carer Signature

I/We give permission for: ……..............................(child's name) ………..(class)
to access the internet and to follow the On-line Safety rules, as set out above, whilst supporting the safe use of Computing at Banstead Community Junior School.

Parent/Carer Signature: …………………………………………………….

Date: …………………………………

Appendix 2

BANSTEAD COMMUNITY JUNIOR SCHOOL

Acceptable Use Policy / Computing Code of Conduct

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of computing. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with Carley Knight, Banstead Community Junior School On-line Safety Leader.

- I appreciate that computing includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that computing use may also include personal computing devices when used for school business.

- I understand that it is a criminal offence to use a school computing system for a purpose not permitted by its owner.

- I will only use my school email account to send and receive school related emails.

- I will only use the school's email / internet / intranet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.

- I will comply with the computing system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that if I share my login details or leave my pc unlocked I am responsible for all activity carried out under my username.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.

- I will only take images of pupils and/or staff for professional purposes on school equipment in line with school policy. I will not distribute images outside the school network without the permission of the Headteacher.

- I will not install any hardware or software without the permission of the On-line Safety Leader/Network Manager.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will respect copyright and intellectual property rights.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

- I will ensure that my on-line activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support the school's Computing and On-line Safety Policy and help pupils to be safe and responsible in their use of computing and related technologies. I will promote on-line safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the On-line Safety Leader, the Designated Child Protection Officer or Headteacher.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of computing throughout the school.

Full Name………………………………………………………………………………
(Printed)

Job title………………………………………………………………………..………………

Signature………………………………………………   Date……………………