On-line Safety Policy

Approved by the PRU Management Committee on:	25th January 2018
Responsible person:	Sunil Vyakaranam
School's annual review date:	March 2020
Next review date:	March 2021 (statutory annual review)

Designated senior person to co-ordinate e-safety Sunil Vyakaranam

Designated senior person for safeguarding Sunil Vyakaranam

Related documents

Safeguarding
Anti Bullying
Teacher standards
Support Staff code of conduct

1. Introduction

1.1 The management Committee of City of Birmingham School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy will be reviewed annually in the light of guidance from the local authority. It will be reviewed earlier if the local authority issues further guidance regarding particular circumstances or developments in information and communication technology.

2. Basic principles

2.1 In adopting this policy the Management Committee has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by Management Committee Members.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, Management Committee Members, visitors and community users who have access to, and are users of, the school's information and

communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The Management Committee expects the head teacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this Management Committee for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the School's policy and procedures for safeguarding children. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The Management Committee expects the head teacher to arrange for this policy to be published on the school website so that it is available to all employees and volunteers in the school. It also expects instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Management Committee

3.1 The Management Committee will consider and ratify this e-safety policy, and review it annually. Management Committee Members are expected to follow the policy in the same way as staff and volunteers are expected to follow it, including participating in e-safety training if they use information and communication technology in their capacity as Management Committee Members.

3.2 Management Committee Members are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head teacher

3.3 The head teacher is responsible for ensuring that

- the Management Committee is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including those on Safeguarding, Bullying and Pupil Behaviour, take account of this e-safety policy
- the Management Committee is given necessary advice on securing appropriate information and communication technology systems
- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy
- the school has a designated senior person to co-ordinate e-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding

- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs
- the school provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and school Management Committee Members who use information and communication technology in their capacity as volunteers or Management Committee Members
- pupils are taught e-safety as an essential part of the curriculum
- the senior management team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem
- records are kept of all e-safety incidents and that these are reported to the senior leadership team
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems
- there is appropriate supervision of, and support for, technical staff
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the head teacher commensurate with their salary grade and job descriptions
- participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum
- using information and communication technology in accordance with this policy and the training provided
- reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including Management Committee Members, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum
- use information and communication technology in accordance with this policy and the training provided
- report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their passwords and they should not write it down or store it where it is possible that another person might discover or steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

4.2 Employees, volunteers and Management Committee Members should:

- not open, copy, remove or alter any other user's files without that person's express permission
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians. The appropriate 'release' form must be completed.
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems

- if they occupy a senior post in which they need to keep e-mail and other messages confidential, they should ask the school for a separate e-mail address for this purpose
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted
- not use personal social networking sites through the school's information and communication technology systems
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems
- not deliberately disable or damage any information and communication technology equipment
- report any damage or faults to the appropriate member of staff using the help desk system
- At least weekly to plug in laptops to the network so that security and other downloads can be updated.

4.3 Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

5. Education and training

5.1 Education and training in e-safety will be given high priority across the school.

5.2 The education of pupils in e-safety is an essential part of the school's e-safety provision and will be included in all parts of the curriculum.

5.3 The school will offer education and information to parents, carers and community users of the school about e-safety.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

5.5 Volunteers and Management Committee Members who use information and communication technology during their work will be offered the same training as employees.

6. Data Protection

6.1 The school will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of the school's data protection policy, including the requirement for secure storage of information.

7. Technical aspects of e-safety

7.1 The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

7.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

7.4 In City of Birmingham School all internet usage is monitored by SmoothWall. Users are reminded of this when logging on to any COBS machine. The school's systems also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

7.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

8. Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported following the procedure in the Safeguarding policy.

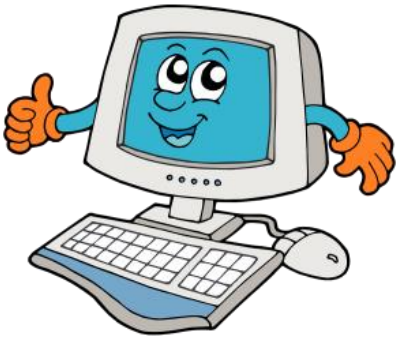
8.2 Any suspicions of other illegal activity should be reported to the head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police. Disciplinary procedures may also be instigated.

8.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or other designated member of the senior leadership team for investigation and appropriate action. This

may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

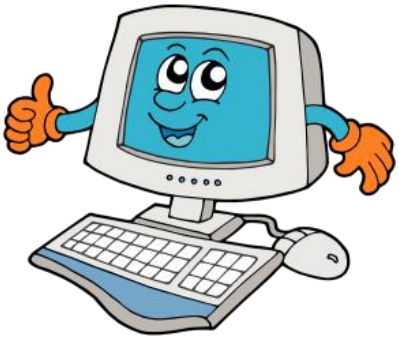
Ready, Respectful and Responsible Internet Use

Using the Computers



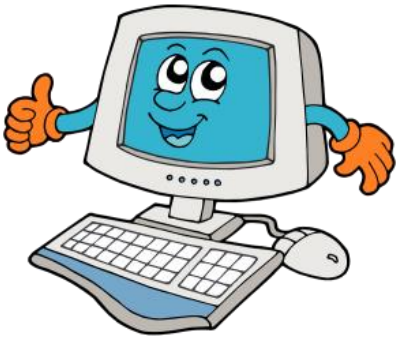
- I will only access the computer system with my own login name and password.
- I will not access other people's files
- I will not bring in Flash Drives, USB memory sticks, or CD ROMs from outside school to use on the school computers without permission.

Using the Internet



- I will ask permission from a teacher before using the Internet.
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

Using e-mail



- I will ask permission from a teacher before checking e-mail.
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself.
- I understand that others may read e-mail messages I receive or send.
- The messages I send will be polite and responsible.
- I will only e-mail people I know, or my teacher has approved.
- I will never give my full name, home address or telephone number in e-mail.
- I will not use e-mail to arrange to meet someone outside school hours.

Internet Usage Agreement

All pupils and their parents/carers will be asked to read and sign this agreement covering the expectations that we have of pupils using the Internet in Centre and regarding the use of photographs.

The Pupil Internet Agreement

This is to be read through with your parent/carer and then signed. You will be allowed Internet access after this is returned to the Centre.

- We expect pupils to be responsible for their own behaviour on the Internet, just as they would anywhere else in the Centre. This includes the materials that they choose to access, and the language that they use.
- Pupils should use their own logon to access the BSS network.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupil encounter such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any rude language in their email or other online communications and to contact only people they know or those that the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- Pupils should not access other pupil's files unless permission has been given.
- Computers should only be used for schoolwork or homework unless permission has been granted otherwise.
- No program files may be downloaded from the Internet.
- No CD ROM or USB flash drives may be brought in from home.
- No programs on flash drive or CD ROM should be brought in from home for use in Centre.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone should be made unless this is part of an approved Centre project.

Pupils consistently choosing not to comply with these expectations will be warned, and may be denied access to Internet resources.

I have read through the agreements with my child and agree to these safety restrictions.

Signed……..(Parent/Carer)

Pupil……Date……

Useful resources

For Parents and Children

Bullying Online www.bullying.co.uk
Advice for children, parents and schools

Kidsmart www.kidsmart.org.uk
An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Family Guide Book (DfES recommended www.familyguidebook.com
Information for parents, teachers and pupils

Action for Children http://www.actionforchildren.org.uk/
Expert advice for children, young people and parents.

Safekids www.safekids.com
Family guide to making Internet safe, fun and productive

Grid Club http://www.gridclub.com/
Internet proficiency through online games for KS2.

For Staff

NAACE / BCS www.naace.org (publications section)
A guide for schools prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

Internet Watch Foundation - www.iwf.org.uk
Invites users to report illegal Web sites

Data Protection www.informationcommissioner.gov.uk/
New Web site from the Information Commissioner

Copyright www.templetons.com/brad/copymyths.html
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.

DotSafe – European Internet Safety Project http://dotsafe.eun.org/
A comprehensive site with a wide range of ideas and resources, some based on Kent work.

Grid Club http://www.gridclub.com/
Internet proficiency through online games for KS2, with a free teacher's pack.