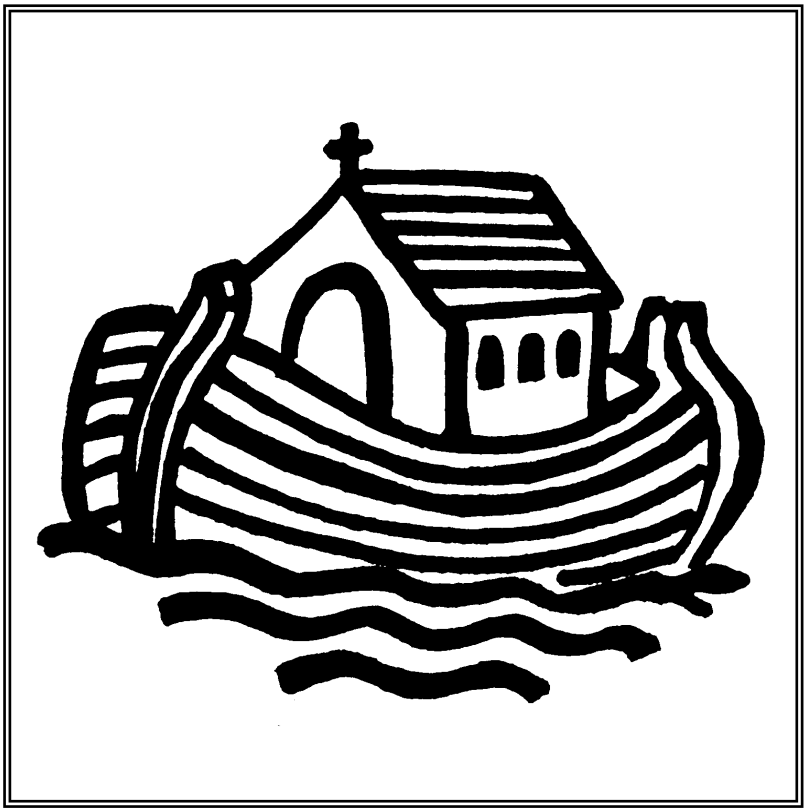
ST BARTHOLOMEW'S C.E. (AIDED) PRIMARY SCHOOL



Acceptable Use of ICT, Data Protection and e-Safety Policy

Written by : Miss H Banks

Date : March 2016

To be read in conjunction with:

- *Child Protection and Safeguarding Policy and Procedures*
- *Mobile Email Access Policy*
- *Staff Code*
- *Social Networking Policy*
- *School Laptop and iPad Agreement for Staff*
- *Computing Curriculum policy*

CONTENTS

1. How will **information systems security** be maintained?

2. How do we keep our **data secure**?

3. How do we manage the use of **pupil images**?

4. How do we manage **published content** (our school **website**)?

5. How do we manage the use of **email**?

6. How will **social networking, social media** and **personal publishing** be managed?

7. How is **internet access** authorised?

8. How will the school respond to any **incidents of concern**?

9. How will the school deal with incidents of **Cyberbullying**?

10. How will **mobile phones** and **personal devices** be managed?

APPENDIX 1: Acceptable Use of ICT Agreement and e-Safety Rules
APPENDIX 2: Parents'/Legal Guardians' Consent to Take and Use Images of Pupils

1. How will information systems security be maintained?

Green data:	Does not identify an individual
Amber data (Sensitive):	Data that will identify an individual by name
Red data (Very sensitive):	Data that includes any personal information e.g. medical, Child Protection etc.

- The server is securely located in an area where children are not permitted.
- Virus protection is installed and managed by the school's ICT Technician.
- The security of the school information systems and users is reviewed regularly.
- Files held on the school's network will be regularly checked.
- The School's ICT technician will review system capacity regularly.

Access to sensitive data is restricted as follows:

T: drive (Teaching resources) - all teachers, TAs and office staff, and SLT
H: drive (one for each member of staff)
S: drive (Shared drive/SIMS) : all teachers, office staff, and SLT
J: drive ('Work' drive) : office staff and SLT

(L: M: N: O: P: Q: R: drives are allocated to year groups and accessible by all staff and all children)

Some folders within these drives containing "red" data are restricted to certain members of staff e.g. the Senior Leadership Team.

Staff H: drives and T: drives should be kept tidy and up to date. They should not contain red data, with the exception of the H: drive of the Designated Safeguarding Lead. Any other data such as pictures and video should be deleted as soon as they are not required. Personal data should not be kept on the school network or equipment; all of the data in your personal H: drive is the property of the school (all data on school machines, laptops and mobile devices is the property of the school).

If you are building a portfolio then you should follow the appropriate policies with regard to photos etc. Never allow others access to your personal H: drive.

The Data Protection Act

The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).

The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual’s rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2. How do we keep our data secure?

- Only school issued encrypted memory sticks are permitted for use in taking data offsite.
- Sensitive data sent over the internet must be encrypted. Senior staff who may need to do this will be trained accordingly.
- No sensitive data will be stored directly onto laptops or workstations.
- Logins and passwords must not be shared with others.
- Passwords should be strong and complex.
- Workstations must be locked when left unattended.
- Users must log off after use.
- Unapproved software is not allowed on workstations.
- Personal devices should not be connected to the school network.
- Personal cameras must not be used for school purposes.

Freedom of Information requests

Requests for personal data will only be accepted in writing and will be responded to within 15 days. Charges may be introduced for large data requests.

3. How do we manage the use of pupil images?

Image taking by parents, legal guardians or family members

- Parents, legal guardians, family members and friends can take images of their child and friends participating in school activities for family and personal use.
- Parents will be asked for their permission via a form when their child joins St Bartholomew's, before photography is allowed.
- Before they are allowed to take images during school activities, parents or legal guardians will be reminded that any images they take must not be used inappropriately and are only for personal use.
- Photography and video filming will be limited to designated areas and must only be for personal use.
- Use of cameras and other equipment will be monitored.

Images for school publications

- The school will only take and use images that are appropriate and are considered to not be open to misuse.
- If an image of a child is used, we will avoid using names.
- If a name is published, no image will be used without specific consent.
- Children and parents should be encouraged to recognise the value of group photographs or recordings of school events.

Images for the school website

- The school will make sure that only appropriate images are used.
- Image filenames will avoid using children’s names.

Webcams

- Webcams are a useful tool for learning. They can allow an individual or class to interact over the internet with others and support links between pupils in different schools, countries and cultures.

- A webcam will only be used in appropriate circumstances such as a normal class setting.

- Both children and adults will be made aware of when a webcam is in use.

CCTV

- The school uses CCTV in some areas of the school property as a security measure. Cameras will only be used in appropriate areas.

Children photographing one another

- Staff will supervise and maintain control over any photography which pupils do during on-school or off-site activities.

- Camera phones are less visible and can be used to bully or take inappropriate images. Children are not permitted to have access to camera phones on site.

- If it is found that cameras or camera phones have been misused, the school will follow its usual disciplinary procedures.

4. How do we manage published content (school website)?

The primary aim of our school website is to disseminate information to current and prospective parents and carers.

- Staff or pupils' personal information will not be published.

- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

5. How do we manage the use of email?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers.
- Access in school to external personal email accounts may be blocked.
- Staff should not use personal email accounts during school hours or for professional purposes.

6. How will social networking, social media and personal publishing be managed?

At present, social media is not accessed in school by pupils. Refer to the Staff Code and the Social Networking Policy for guidance regarding adult use of social networking and social media.

- The school will control access to social media and social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the site before use and check each site's terms and conditions to ensure the site is age appropriate.

- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.

- Members of staff are advised not to run social network spaces for pupil use on a personal basis.

- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

7. How is internet access authorised?

- Pupils will be supervised in their use of the internet.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Brighton and Hove City Council can accept liability for the material accessed, or any consequences resulting from internet use.

8. How will the school respond to any incidents of concern?

e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Safeguarding Lead.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school will determine the level of response necessary for the offence disclosed. The decision to involve Police will be made as soon as possible, after contacting the Child Safeguarding Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child Protection log.
- The Designated Safeguarding Lead will be informed of any eSafety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- Any complaint about staff misuse will be referred to the head teacher.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or e-Safety officer and escalate the concern to the Police.

9. How will the school deal with incidents of Cyberbullying?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.

- All incidents of cyberbullying reported to the school will be recorded, including of details action taken.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully being asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access being suspended at school for the user for a period of time.

- Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour or other policies.

- Parents/carers of pupils will be informed.

- The Police will be contacted if a criminal offence is suspected.

10. How will mobile phones and personal devices be managed?

Pupils' Use of Personal Devices

Children are not permitted to use personal mobile phones on the school premises. Any mobile phones which are brought to school must be handed in to the office at the start of the day, where they are kept in named individual wallets, and be collected at the end of the day. They should be switched off at all times when on school premises.

If a pupil persistently breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office and the child's parents requested to collect the phone.

If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

Staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of school in a professional capacity, unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

Mobile phones and devices will be switched off or switched to ‘silent’ mode, and will not be used during teaching periods or when children are present.

If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. If a member of staff breaches the school policy then disciplinary action may be taken.

Appendix 1

Acceptable Use of ICT Agreement and e-Safety Rules

General

Virus protection software is used and updated on a regular basis.

A member of staff will be appointed as responsible for the school's e-safety.

Pupils' Access to the Internet

St Bartholomew's CE Primary School uses the Brighton and Hove "filtered" internet service, which will minimise the chances of pupils encountering undesirable material. St Bartholomew's CE Primary School will normally only allow children to use the internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils.

Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

Expectations of Pupils using the Internet

All pupils are expected to read through the ICT Agreement with a parent/carer. Parents are asked to sign the agreement on behalf of their child(ren) and return it to the school.

We expect all pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

Pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.

Pupils are expected not to use any rude language in their electronic communications and 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 will not access social networking sites unless expressly permitted by the school or as part of a specific learning activity.

Pupils should not access other people's files unless permission has been given.

Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

No program files may be downloaded to the computer from the internet. This is to prevent corruption of data and avoid viruses.

No programs on disc or other portable media should be brought in from home for use in school.

No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

Uploading and downloading of non-approved software is not permitted.

Personal devices should not be connected to the school internet connection without consent from a member of the Senior Leadership Team.

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

Our School Website

The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.

Photographs of individual children will not be published on the school website without parental permission.

The school website will avoid publishing the full names of individuals in or alongside a photograph.

E-Safety Rules

These rules have been written to make sure that you stay safe when using ICT. This includes the use of PCs, cameras, laptops, microphones and all

other ICT equipment. By using the ICT in school, you have agreed to follow these rules. Your parent/carer will discuss these rules with you and sign them on your behalf.

I will only use ICT in school for my learning;

I will keep my password secret and only share it with my parents and teacher;

I will make sure that all ICT contact with other children and adults is responsible and polite;

I will not use the internet to look for, save or send anything that could be unkind or unsuitable;

I will tell an adult immediately if I find or see anything which makes me feel worried, unsafe or upset;

I will never share personal details when I use the internet (address, full name);

I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety;

I will look after ICT equipment in school;

I will only log on using my own class username;

I will think before I click (saving, deleting, printing).

APPENDIX 2

Parents'/Legal Guardians' Consent to Take and Use Images of Pupils

Dear Parent(s) and Carer(s),

There have been rapid changes in the technology of image reproduction. Taking and publishing pictures is now very easy and it can be difficult for schools to monitor and control images of children.

St. Bartholomew's CE Primary School has a duty to provide a safe environment for pupils at school. While we are aware of the risks of image misuse, we believe that the school needs to balance this against the positive value of professional, high quality images of pupils in celebrating and promoting the school as an enjoyable, colourful and vibrant place to learn. Good pictures of the school and its children can help in putting the school at the heart of the local community and enhance its reputation.

Key Policy Points:
St. Bartholomew's CE Primary School recognises that a balance between the low risk of misuse and the numerous positive results of colourful, well produced school material is necessary.

The school will only take and use images (photographs, videos and DVDs) that are appropriate and are considered to be safe from misuse.

Children will be made aware of why their pictures are being taken and how they will be used.

The school will take extra precautions to ensure that only appropriate images are used for the website.

If it is found that a camera phone has been misused the school will follow its usual disciplinary procedures.

If an image of a child is used, we will avoid using the child's name. If a name is published, no image will be used without specific consent.

Parents and legal guardians will be asked to sign an agreement that any images they take during school activities will not be used inappropriately.

Please read the policy carefully and fully, and return it to indicate that you agree with the school's policy and consent to images of your child being taken and published in school material and Brighton & Hove Council publications.

St. Bartholomew's CE Primary School’s policy is to allow parents to take images of their children during school activities. Please read the parental consent form and sign the agreement for responsible use of images you intend taking during school events.

Yours sincerely
Headteacher

Parents'/Legal Guardians' Consent to Take and Use Images of Pupils

Please read the letter overleaf and indicate whether you agree to your child's images being taken.

You have the option to indicate whether or not you consent to your child's images being taken and used for different purposes (these include photographs and video).

Name of child (block capitals):
Name of parent or legal guardian (block capitals):

I have read the school's key policy points on the use of images of children and I agree to its provisions.

Please give your consent by putting your initials next to each statement.

Your child's images will not be taken/used as specified, if you do not give your consent.

Please tick the boxes to the right beside each statement

I give my consent to images of my child being taken and used for official school purposes of promoting or publicising school events in accordance with the guidelines of the policy for the duration of their time at the school.

I give my consent to images of my child being used on the school website and I understand that these images will be available on the World Wide Web.

I give my consent for images taken by the school in accordance with the guidelines of the policy to be used for official Brighton & Hove Council publications.

I give my consent to images of my child being taken and used by the press at school events e.g. The Argus.

I give my consent to my child being included in any images taken by other parents or carers who wish to photograph or record school events in which their children are participating. All parents or legal guardians will be asked to sign an agreement for appropriate use of images they take during school events - please
see below.

I agree that any photographic or video images I as a parent or legal guardian might take at school events will not be used inappropriately unless it is only my child(ren) in the photograph (e.g. shared via social networking such as Facebook)

Signature of parent or legal guardian of the child:

Date:

NB: There may be other circumstances, falling outside the normal day to day activities of the school, when images of children are needed. The school recognises that in such circumstances specific consent from the parent or legal guardian will be sought before any photography or filming of children starts. If you have concerns or queries about any of this information, please contact the school.