Bishop Bridgeman Church of England Primary School

Acceptable Users Policy

The school's Acceptable Use Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The computer system is owned by the school, and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school computer system is taken to mean all computers owned by the school – on site and off site desk top units and lap tops.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff requesting computer access should sign a copy of this Acceptable Use Statement and return it to the ICT Curriculum Group for approval.

General Use

- All Internet activity should be appropriate to staff professional activity or the pupils education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Use of the network to access inappropriate materials such as 'adult', racist or offensive material is forbidden and may result in dismissal.

E-mail

- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Never share your e-mail address with current or past pupils.
- Never send or respond to an e-mail sent by a pupil.

Classroom computers

- When leaving room lock computer so children cannot access confidential files located on P:drive or SIMS. Do this by holding down Ctrl Alt and Del buttons then selecting lock computer. To unlock, just enter your log on details and password. This should also be done in the ICT suite if logged on and leaving the room without logging off.
- Never log onto a computer or the CLC for a child using your user name or password as they can access confidential information stored within P:drive.

Pen Drives

- Whenever possible try not to leave a pen drive visible e.g. in computer when leaving a room.
- When saving any file to your pen drive containing children's names or result data, including reports and trackers, ensure they are password protected. To do this on a Microsoft Office Application such as Word click the office button, prepare the select encrypt document. Enter password. Each time this file is accessed it will now ask for this password (See attached how to document)

Social Networking Sites

- Never invite or accept current or past pupils and parents to share personal details on social networking sites. All children under the age of 13 requesting friendship on such sites must be reported to the site and the e-safety co-ordinator within school.
- Never hold online discussions with current or past pupils and parents.
- Use professional judgement when publishing personal photographs and status details on such sites – do you really need to mention work?
- Ensure any social network accounts you may have are only accessible to friends and are not public
- Remove address and place of work from your homepage.

Cameras/photographs

- If using a personal camera from home ensure that all personal photographs have been deleted before using in school.
- Never take photographs of children home – on a camera, pen drive or printed out.

Mobile Phones

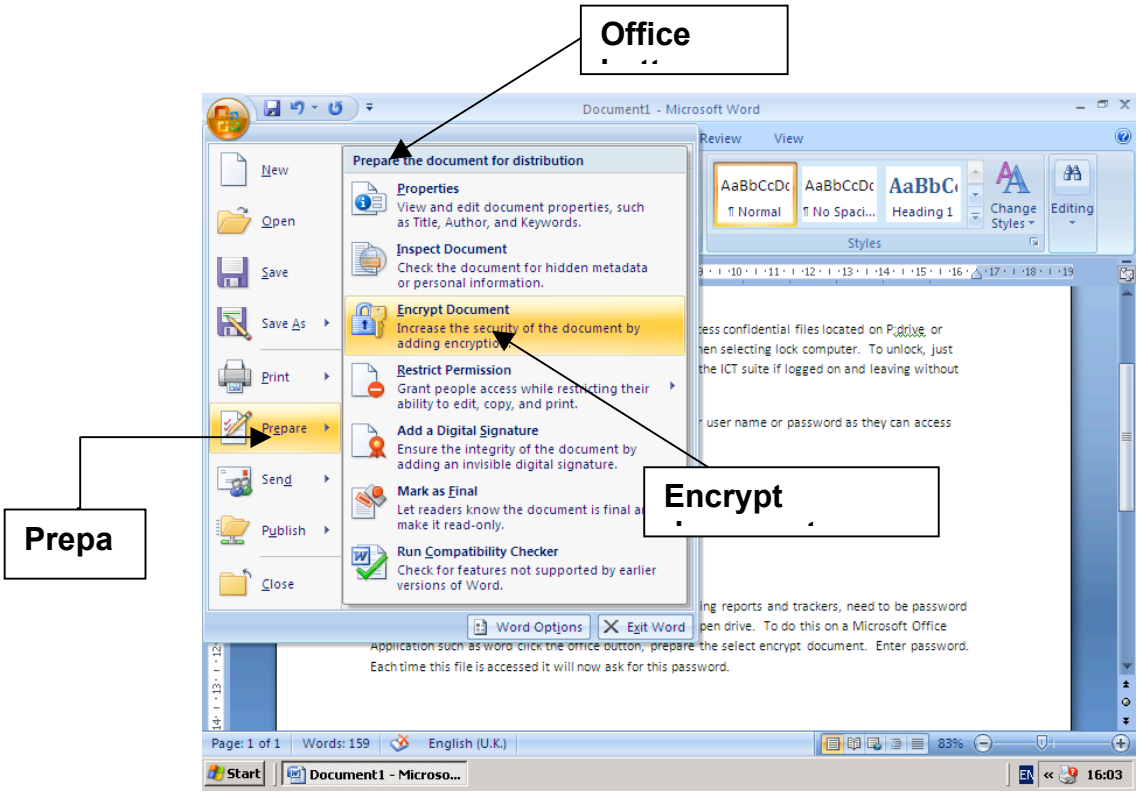
- All mobile phones should be switched off or on 'Silent' during the school day.
- Do not use your phone within the classroom during the school day unless it is an emergency. All emergency contacts should be the school office number.
- Turn off your Blue tooth or password protect it.
- Never take a photograph for school use on your phone.

Internet Searches including Google Images

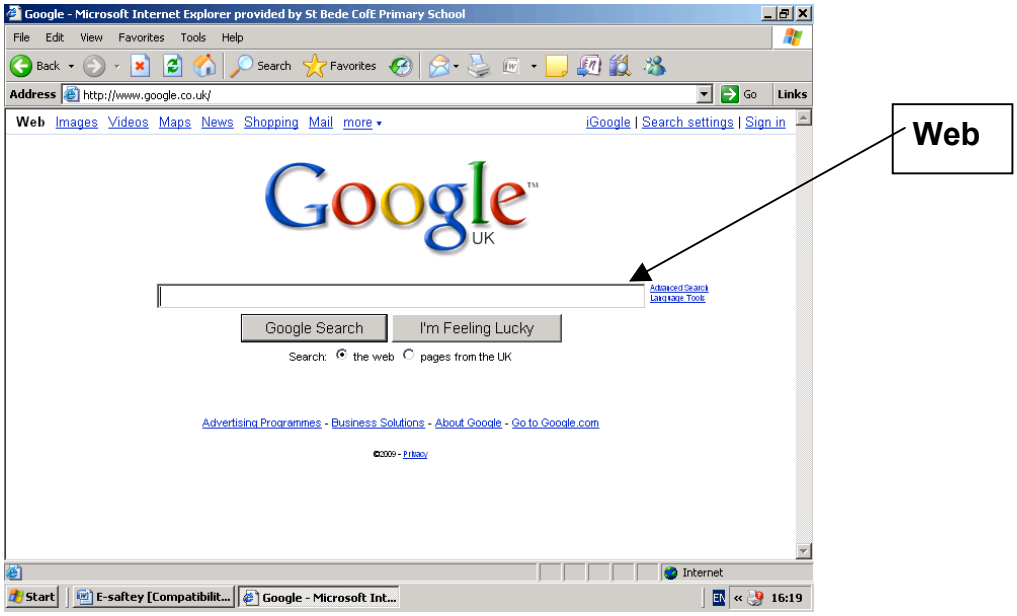
- Ensure that all searches conducted in front of children have been planned for and previously checked.
- Children are no longer allowed to use Google Images to search for images as firewalls do not block inappropriate images. Teach children to search 'web' then click on a website to find the picture.

HOW TO…

How to password protect an office document



How to search the web rather than using Images



Reviewed: September 2016

Next Review Date: September 2017