St Bede C of E Primary Academy and St Bede's Childcare Limited & PAL Limited

Acceptable Use Policy

(Networking, Communications and Recording Devices)

All staff should sign this statement and return it to HR in the Administration office

For the purposes of this document the term 'the school' shall mean and include St. Bede C E Primary Academy, St. Bede's Childcare Ltd and PAL Limited. SMT refers to the Senior Management Team and SCT refers to the Senior Childcare Team.

This policy has been drawn up to protect all parties - pupils, children, staff and the school.

The computer system is owned by the school and may be used by pupils/children to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The system is taken to mean all computers or equipment (computers/desk tops/lap tops/tablets/smart phones or any device supplied by the school) – both on site and off site.

The school reserves the right to monitor, examine or delete any files held on its computer system and monitor, examine or delete any internet sites visited.

In addition to the contents of this policy all staff must comply with all current legislation governing those who work with children and young people.

General use

- All Internet activity should be appropriate to staff professional activity or 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;
- at the complete discretion of the school any wilful use of the network to access inappropriate materials such as 'adult', pornographic, racist or offensive material is forbidden and will result in dismissal;
- please be cautious of any email or website that could create contamination of the systems via a virus.

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;
- it is strictly prohibited to share your e-mail address with current or past pupils/children;
- it is strictly prohibited to send or respond to an e-mail sent by a pupil/children;
- please be aware that the school owns any communication sent via email or that is stored on its equipment and the School has the right to access and monitor any communications.

Classroom computers

- When leaving a room lock computers so pupils/children cannot access confidential files located on P:drive or Bromcom (so no-one can access confidential information located on the system). Do this by holding down Ctrl Alt and Del buttons then selecting lock computer. To unlock, enter your log-on details and password. This also applies in the ICT suite if logged on and leaving the room without logging off;
- never log onto a computer or the VLE for pupils/children using your user name or password as they can access confidential information stored within P:drive.

Off-site data access

The method of transferring data between school and home is via the VPN system. Details and set up instructions are provided by the IT department. If using a pen drive this must be encrypted. Always remove a pen drive when leaving a room. When saving a file to a pen drive containing pupils/children's names or result data, reports and trackers, they must be password protected.

Social media networking sites

- It is strictly prohibited to invite or accept current or past pupils/children and parents to share personal details on social networking sites. All pupils/children under the age of 13 requesting friendship/contact on such sites must be reported to the site and the e-safety co-ordinator within School (Beth Garvey);
- it is strictly prohibited to hold online discussions with current or past pupils/children or parents;
- use professional judgement and discretion when publishing personal photographs and status details on such sites. Comments relating to work must be kept to a minimum and should be appropriate and positive. Negative comments which clearly relate to work should not be made. This includes 'liking' other people's statuses or tweets, agreeing with negative work related comments;
- status updates or tweets during working hours (i.e. during breaks or lunch) are indicative of your feelings whilst at work and their content should be considered and appropriate;
- ensure all personal social network accounts you have are only accessible to friends and not public;
- remove address and place of work from your homepage;
- social networking sites should not be accessed from the school's system;
- nothing which contains or identifies the school or its logos must be published on any social media website.

Electronic devices

The use of any electronic device which has the ability to capture or record data from the school's computer system is to be used strictly for the purpose of and benefit of the school. Use for any other purpose is strictly prohibited.

Cameras/photographs*

- If using a personal camera ensure all personal photographs have been deleted before use in school;
- it is strictly prohibited to take photographs of pupils/children home – on a camera, pen drive or any other device or printed out;
- iPads must only be used by pupils/children under the supervision of a member of staff.

Mobile phones*

- All personal mobile phones should be switched off or on 'silent' during the school or working day;
- do not use your personal phone within a 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 personal phone;
- it is strictly prohibited to place anything on the internet from your phone.

*Consent may be given to photographing/recording on personal devices with the written consent of a member of the SMT/SCT team. If consent is given data must be deleted after use and confirmed to the SMT/SCT team (see *Appendix A* – forms are available in the SMT Office and SCT Office).

Internet searches including Google images

- Ensure all searches conducted in front of pupils/children have been planned for and previously checked;
- pupils/children are protected when searching the internet by the St. Bede Safesearch, which blocks any inappropriate images or content;
- any YouTube content being used by the staff with pupils/children must be checked from beginning to end by staff before use;
- it is strictly prohibited to place anything on the internet relating to school.

All staff should be mindful of their duty to report any concerns they may have relating to any other member of staff, which is deemed inappropriate or unprofessional.

Full name: _____

Signed: _____ **Date:** _____

Any person in breach of the above policy will be subject to disciplinary proceedings