Acceptable Use Policy (Staff)

Introduction
The facilities of the Beechwood computer networks are provided as an aid to teaching and the general operation of the School.

You are encouraged to contribute to the above by:

- Learning how to use ICT effectively. This includes accessing the Internet, e-mail, 3Sys and the use of equipment such as electronic whiteboards and projectors.
- Using the Internet and information sources such as web sites and other multi-media to research subjects when preparing curriculum material.
- Using the ICT facilities to undertake your own Continuing Professional Development and studies of your own interests.
- Using the School network to share information, practice, course material(s) with colleagues within Beechwood and, where appropriate, other schools.

All members of staff are provided with access to the School's Network and the Internet and e-mail.

All members of staff are provided with a secure School e-mail account which is setup on the School's network.

Staff may use the School's ICT services for personal use provided it does not impact on their duties, put the School at risk and the volume is not so great as to disrupt the use of the Network and its facilities (i.e. printing).

This policy should be read in conjunction with the school's Safeguarding policy, with reference to the Prevent Duty (June 2015) which addresses online radicalisation and the Staff Code of Conduct as well as the school's GDPR Policy.

Acceptable Use
In using the Beechwood's ICT services, e.g., its Network, applications, the Internet, 3SYS and the e-mail facilities **you are required to:**

- Abide by the Policy described outlined in this document.
- Keep your Network password(s) secret and make sure that they are not guessable — note that if pupils obtain your password they can gain access to your personal data, and the data stored in shared staff data areas on the network. There is also a risk that they can access confidential data. Under the Data Protection Act and the GDPR Policy, you have the responsibility of ensuring that data under your control is protected against misuse.
- Respect copyright and/or license agreement on material stored on the Internet, sent by e-mail and made available on CD's and other software.
- Be aware when sending e-mails from a School e-mail address that the contents may be mistaken as representing the policy/position of the School and so care needs to be taken to compose your e-mails accordingly.
- Allow the anti-virus software installed on School computers to check all incoming files.

- Only use the Beechwood e-mail for communication with pupils. Similarly, all School related business (communication with parents, staff, outside agencies) should be undertaken using the School's email (Outlook Webmail). This is to protect your own privacy and that of the School.
- Ensure that you log out at all times.

Do not:

- Access, produce or transmit material that is: offensive, threatening, obscene, blasphemous, hateful, racist, defamatory or material which could suggest an interest in radicalisation. Accessing such material for academic research must be undertaken with extreme caution and even then, subject to the necessary authorisation.
- Use the Network for any commercial enterprise not connected with the School and its authorised activities.
- Use the Internet to order items on behalf of the School or otherwise contractually commit the School without the correct authority.
- Download from the Internet or from email any program or attempt to install any program on any School computer. Where you feel a piece of software would be valuable to you, please consult the ICT Department first in order to obtain the necessary systems permissions. Where there is disagreement the Head or Deputy Head will make a final decision.
- Accept invitations or and/or requests from students to partake in discussion forums, instant messaging and webcams. If you are unsure do check first with the Head or the Deputy Head.

I-Pad Use Policy

I-Pads are available as a convenience to staff in the execution of their School duties.
I-Pads may be taken away from the School, but caution must be exercised to ensure the physical security of the I-pad as well as the data contained therein. I-Pads should not be left so that they are a temptation to others. The need to secure your password, what may or may not be downloaded, together with the other advice outlined in this document applies to I-Pads. All class I-Pads are numbered. When using the I-Pads all staff must write down the number of the I-Pad so that there is a record of which child has used which I-Pad. Staff must remind students to log off each I-Pad at the end of the session. This is a safeguarding issue.

Mobile Phones

Mobile phones can only be used during non-contact time. It can be kept on silent mode during lessons except in an emergency and then with the agreement of the Deputy Head or the Head.

Do not use your personal mobile phone or other personal electronic equipment to photograph or video pupils or staff without permission from the Head or Deputy Head. Do not use your personal phone to photograph or text students.

General

Should the use of instant messaging, chat rooms, webcams or discussion forums for communicating with pupils or parents about learning be necessary, it will only be via the School's network and with permission from the Head or Deputy Head.

As a member of a staff you will take all reasonable steps to ensure the safety and security of school ICT equipment which is taken off site and will remove anything of a personal nature before it is returned to School.

As a member of staff you will take all reasonable steps to ensure that all ancillary devices, e.g., memory devices are fully virus protected and that protection is kept up to date. All devices brought in to school which are being used for Wi Fi access must be taken to the IT Department to avoid the device being blocked or shut down.

As a member of staff you will report any accidental access to material which might be considered unacceptable immediately to the Deputy Head/DSL this may include pornography or violent material taking in to

consideration the Prevent Duty (June 2015) You will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Beechwood community.

Monitoring

The School monitors and blocks inappropriate internet and e-mail traffic via a system called Securus and Impero. Please be aware that the School's internet security responds to key words. Words that are deemed by the software to be of concern are captured in a screenshot.

Access to internet websites offering web based e-mail is allowed but we would ask you to be very careful with the use of web-based mail. These sites are potentially insecure and do not offer adequate e-mail virus protection therefore exposing the School's ICT Network, as well as your personal data, to unnecessary risk.

Personal devices are not currently supported by the School's network although personal computers can connect wirelessly in certain parts of the School which will require a Network code. If you wish to have a personal computer or I-pad supported by the Network this can be done subject to the protocols and guidance laid out in this document.

Any suspected breach of the above Policy will prompt notification to the user; after which, and with the authority and permission of the Head, the IT administration staff will have the right to inspect personal data and e-mail folders.

The School, as part of the data backup process, will copy and retain all School files and folders saved in the designated Network share, together with the e-mail files stored within the School e-mail system purely for data recovery procedures /purposes.

Reviewed September 2019 (DHM).
To be reviewed September 2020.