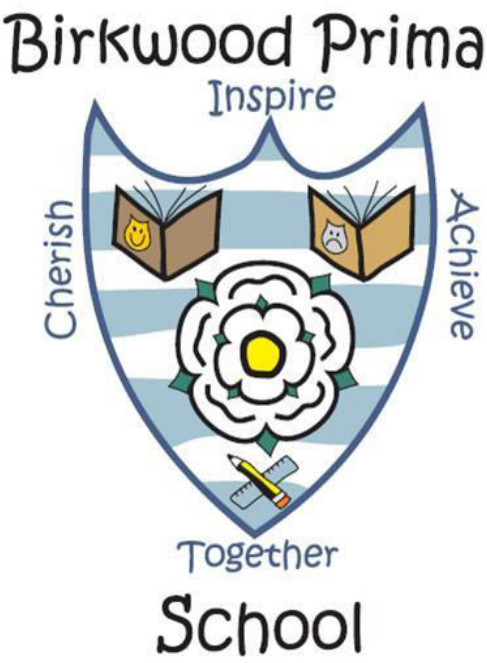

ACCEPTABLE USE POLICY

UPDATED FEBRUARY 2022

Background
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. In order to ensure the security of school systems and data the school will ensure that:
    - all devices have the latest OS software installed
    - devices which are no longer required are totally wiped (factory reset) before being sold or given to another person
    - Only verified apps are installed onto devices
    - 2 factor authorisation is used to access school based emails

The school will ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Staff Acceptable Use Policy Agreement
As a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, iPadS, email and social media sites**.**
- I understand that any personal device I may use to access school data must have the latest OS software installed.
- I understand that I must not use any 'jailbroken' device to access school system or data. (Jailbreaking removes restrictions within a devise operating system meaning that they can run software and do things that are normally not allowed).
- When I change a device that has school systems installed, I will ensure that they are totally wiped (factory reset) before they are sold or given to another person.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Lead.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones).
- I will respect copyright and intellectual property rights and will gain necessary permissions where required.

- I have read and understood the school Online Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Bursar.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Team (Code Green) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- When sending school emails to outside agencies/contacts, I will ensure encryption is used to protect email content and data. I will ensure that emails are sent to the correct person, if errors occur I will report these to the Bursar.
- I will not open any attachments to emails if the source is not known and trusted.
- I will ensure that my school email is not set up on a personal device unless 2 factor authentication is used i.e. in addition to my phone pin/password, an email login/security passcode is required.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Headteacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

Birkwood Primary School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Staff are expected to agree and comply with the Staff ICT Acceptable Use Policy.

Monitoring and Review

The Governing Body reviews this policy every 2 years. The Governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the governing body receives recommendations on how the policy might be improved.

This policy will be reviewed in February 2024.

Signed _____ Headteacher Date _____

Signed _____Chair of Governors Date _____