Code of Conduct for the Acceptable Use of Information Technology - **Staff**

Information Technology and related technologies, such as computers, interactive whiteboards, e-mail, the Internet and mobile devices, are an expected part of our daily working life in school. This Code of Conduct is based on the main statements concerning members of staff which form part of the school's E-Safety Policy and Safer Working Practice Guidance.

To ensure that members of staff are fully aware of their professional responsibilities when using any form of IT, all staff are expected to comply with this Code of Conduct. Any concerns or clarification should be discussed with the Headteacher or DCPO's.

I understand that

- IT includes a wide range of systems, including; computer networks, laptops, mobile phones, PDAs, digital cameras, e-mail, social network sites, learning and meeting platforms, and the Internet.
- It may be a criminal offence to use a school IT system for purposes not permitted by its owner.
- Failure to comply with this Code of Conduct may result in sanctions being imposed, formal disciplinary action being taken or illegal use being reported to the appropriate authorities.
- All my use of any school computer network and the Internet will be monitored and logged.
- The school will exercise its right to monitor my use of the school's IT systems, including; hardware, software, Internet access and e-mail.
- The Headteacher may designate a member of staff to delete any of my files, including e-mail, where they believe that unauthorised use of the school's information system may be taking place, or it may be being used for illegal purposes.
- Digital copies of images of pupils/staff/parents/carers may only be taken, stored and used for professional purposes, in-line with the school's policy on the taking and use of photographs.
- Digital copies of images of pupils/staff/parents/carers must not be e-mailed or distributed outside the school without the permission of the Headteacher.
- Staff will not take photographs of children on mobile phones.
- Staff will not use mobile phones during directed time, i.e. contracted hours (permissible during break times only, away from children) unless authorised by the Headteacher.

I will

- Adhere to all the schools' Safeguarding Policies and Procedures at all times
- Comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- Only use the school's IT systems (including; hardware, software, email, Internet, Intranet, learning and meeting platforms, Google Drive) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Academy Council.
- Ensure that all electronic communications with pupils, parents and staff are compatible with my professional role.

- Take all reasonable steps to ensure that school data is stored securely and used appropriately, whether in school, taken off school premises (using an encrypted storage device) or accessed remotely.
- Respect copyright and intellectual property rights.
- Adhere to GDPR legislation.
- Support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of IT and related technologies.
- Report any accidental misuse of school IT, or accidental access to inappropriate material, to the E-Safety Leader or Headteacher.
- Immediately inform the Headteacher if I receive any offensive e-mail.
- Report any incidents of concern regarding children's safe use of IT to the E-Safety Leader, DCPO's or Headteacher.

I will not

- Use any school IT for any purpose that could be deemed illegal, inappropriate, unprofessional, racist, hateful, or harassment.
- Browse, download, upload or distribute any material that could be considered offensive, pornographic, obscene, illegal or discriminatory.
- Undertake any private business activities of any nature using school IT.
- Allow anyone else to use a computer when I have logged on using my own username.
- Allow anyone else to use my username and password.
- Deliberately circumvent the school or internet security and filtering systems.
- Use YouTube, or similar websites live, when pupils are present, or encourage pupils to use them at school or home. All websites must be vetted prior to use with the children to ensure the content is appropriate.
- Use Facebook or similar websites when pupils are present, or encourage pupils to use them at school or home.
- Communicate with parents/carers or pupils via social networking sites (such as Facebook) or accept them as their "friends".
- Access the internet other than through the school's security systems whilst on school premises.
- Install any hardware or software without permission from the Headteacher.
- Connect any personal laptop, digital camera or other device, to any school system unless it has up-to-date antivirus protection.
- Use my mobile phone during directed time, i.e. contracted hours (permissible during break times only, away from children) with the permission of the Headteacher
- Take photographs of children on mobile phones.

I have read and understood the school's CP and Safeguarding Policy and Safer Working Guidance.
I agree to comply with this code of conduct.

Failure to do so may lead to disciplinary action. All behaviour must be in-line with the Safer Working Practice Guidance.

Laws which may apply: Computer Misuse Act 1990, Data Protection Act 1998, Communications Act 2003, Copyright Design and Patents Act 1988, Malicious Communications Act 1988, Obscene Publications Act 1959 and 1964, Racial and Religious Hatred Act 2006, Sexual Offences Act 2003, The Telecommunications (Lawful Business Practice -Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Protection from Harassment Act 1997, Public Order Act 1986, Human Rights Act 1998, Protection of Children Act 1978.

Staff name: ……. Staff signature: …… Date: ……