Austhorpe Primary School

Acceptable Use of IT for Staff 2025-26

Date of Policy: September 2025

Austhorpe Primary School

Acceptable Use of IT for Staff September 2025

IT 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. To ensure members of staff are fully aware of their professional responsibilities when using any form of IT all staff are expected to comply with and sign this code of conduct. Any concerns or clarifications should be discussed with the Headteacher.

I understand that:

- IT includes a wide range of systems including computer networks, laptops, mobile phones, PDAs, digital cameras, iPad, e-mail, smart watches and the internet
- It may be a criminal offence to use school IT equipment for purposes not permitted by its owner (Red Kite Learning Trust)
- 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 uses of the school computer network and the network will be logged.
- The school may exercise its right to monitor any 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 systems may be taking place, or it may be used for illegal purposes
- Digital copies of images of pupils and/or staff may only be taken, stored and used for professional purposes on school owned equipment only, in line with the school's policy on digital images (Safer Working Practice.) Digital copies of the pupils and/or staff must not be e-mailed or distributed outside the school without permission from the Headteacher.
- All searches go through our robust filtering system and this generates a daily alert to the headteacher and DSL

I will:

- Comply with the school IT system security and not disclose the passwords provided to me by the school or other related authorities
- Only use the school's IT systems (including hardware, software, e-mail, internet, network & learning platform) and any related technologies for appropriate purposes
- Ensure that all electronic communications with pupils, parents and staff are compatible with my professional role and are not deemed illegal, inappropriate, unprofessional, racist, hateful or harassment
- Take all reasonable steps to ensure that school data is stored securely and used appropriately, whether in school, taken off premises of accessed remotely e.g. via the portal
- Respect copyright and intellectual property rights
- 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 including providing adequate supervision of pupils using IT
- Report any accidental misuse of school IT, or accidental access to inappropriate materials to the Headteacher
- Immediately inform the Headteacher if I receive an offensive e-mail or offensive information on any social media

- Report any incidents of concern regarding children's safe use of IT to the Child Protection Designated Lead or the Headteacher as appropriate
- Thoroughly check downloaded or web-based resources (e.g. YouTube clips other video clips streamed from the internet, Web search engine results and web page content and links) before using them with pupils
- Be responsible for everything accessed, used or saved on any IT equipment belonging to school
- Conform to May 19 Guidance to Safer Working Practice, amended in Feb 22, with especial notice to sections 6 and 12 (3G/4G/5G agreed to be used in 'safe places' only within school – staffrooms, offices- and never to be accessed in central areas); this includes use of smart watches
- Immediately inform the DPO (data protection officer) dataservices@judicium.com and the headteacher of any data breach
- Follow the 4Cs of online risk and harm (Content, Conduct, Contact and Contract risks), that is referenced in the Online Safety Policy
- Inform RKLT Helpdesk if unsuitable material is allowed to be viewed/accessed on a device by adult or child so it can be blocked
- Ensure all access to the internet – on school devices or personal devices - is appropriate for the profession

With regard to AI, I will:

- use AI in accordance with the Trust AI Policy and the systems established by the Trust.
- Before using any AI system, I must:
  consult the AI Register
  confirm that the AI tool is listed and approved for the intended use
  familiarise myself with the permitted uses and any restrictions recorded in the AI Register
- attend training provided by the Trust
- understand that AI is a support tool designed to enhance teaching and delivery but is never a substitute for professional judgement.
- understand that the quality and content of any final material(s) remains my responsibility.
- remain responsible and accountable for the accuracy, appropriateness and quality of any AI-generated material I use or adapt, including in contexts such as:
  creating or adapting educational resources
  planning lessons or curriculum content
  drafting tailored feedback or revision materials
  supporting administrative tasks such as report writing or meeting preparation
- uphold all relevant legal and regulatory standards when using AI, including:
  data protection and UK GDPR
  copyright and intellectual property rights
  equality legislation
  my duties under Keeping Children Safe in Education

I will not:

- Use any school IT for purposes that might be deemed illegal, inappropriate, unprofessional, racist, hateful or harassment or in ways that cause anxiety or offence to others
- Disclose the password for my iPad/laptop to pupils.
- 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 when using school IT.
- Allow anyone else to use a computer or iPad when I have logged on using my own username or password

- Allow anyone else to use my username and password
- Deliberately circumvent the school's security and filtering systems
- Allow pupils' access to school's network through my own username and password
- Use social media in public places or access
- Install any hardware or software without permission from the Headteacher
- Install social media on my iPad other than for educational purposes
- Connect any personal laptop, digital camera or other device to any school system unless it has up to date virus protection
- Use any social media to make comments about school or any member of school staff
- Use AI systems to make decisions that carry significant consequences for pupils or staff (e.g. safeguarding, behaviour, performance, SEND)
  to assess subjective work without applying their own professional judgment
  to impersonate others or present AI-generated work as wholly human-authored
  for any purpose that is unlawful, misleading or outside the scope of approved use

I agree to comply with this code of conduct for the academic year 2025-26

Signature…… Date……

Full name (printed)……

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 Act (Lawful Business Practice- Interception of communications) Regulations 2000, Regulations of Investigatory Powers Act 2000, Protection of Harassment Act 1997, Public Order Act 1986, Human Right Act 1998, Protection of Children's Act 1978, Defamation Act; GDPR guidance 2019