Woodsetton School

IT and Acceptable Use policy (staff)

Approved by: **K Hermon**		**Date:** October 2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

1. Purpose

Information and Communication Technology (ICT) plays a vital role in teaching, learning, safeguarding, communication and the efficient operation of the school. This policy sets out the standards and expectations for all staff when using school ICT systems, devices, networks, internet services, software and digital resources.

The purpose of this policy is to:

- Promote the safe, secure and responsible use of technology.
- Protect pupils, staff and the wider school community.
- Support effective teaching, learning and administration.
- Ensure compliance with safeguarding, data protection and cyber security requirements.
- Maintain the integrity, security and reputation of the school.
- Support staff in using digital technologies professionally and ethically.

2. Scope

This policy applies to:

- All employees.
- Agency and supply staff.
- Governors and Trustees.
- Volunteers.
- Contractors.
- Trainees and students.
- Any adult granted access to school ICT systems.

This policy applies wherever school systems are accessed, including on school premises, at home, during educational visits, and in any other location.

3. Staff Responsibilities

All staff are expected to:

- Use school ICT systems professionally and responsibly.
- Follow all safeguarding, data protection and information security requirements.
- Protect confidential information relating to pupils, families and staff.
- Act as positive role models in the use of technology.
- Report concerns, incidents or breaches immediately.
- Use professional judgement when using technology to support their role.

Failure to comply with this policy may result in disciplinary action.

4. Professional Conduct

Staff must:

- Use ICT resources primarily for educational and school business purposes.
- Ensure all digital communication is professional and appropriate.
- Treat others with respect in all online interactions.
- Protect the school's reputation in all online activities.
- Maintain appropriate professional boundaries with pupils and families.

Staff must not:

- Use school systems for illegal, offensive, discriminatory or harassing activities.
- Engage in online behaviour that could bring the school into disrepute.
- Access or share inappropriate material.
- Use technology in a way that compromises safeguarding.

DRAFT

5. Safeguarding and Online Safety

Safeguarding remains paramount when using technology.

Staff must:

- Follow the school's Safeguarding and Child Protection Policy at all times.
- Report any safeguarding concerns immediately through established reporting procedures.
- Report exposure to harmful, extremist, illegal or inappropriate online content.
- Maintain professional boundaries when communicating with pupils and families.
- Challenge and report online behaviours that place children at risk.

Staff must not:

- Communicate with pupils using personal social media accounts.
- Use personal messaging applications to contact pupils.
- Accept friend requests or follow requests from current pupils.
- Share personal contact details with pupils.

6. Use of School Equipment

School devices remain the property of the school.

Staff must:

- Take reasonable care of all equipment.
- Keep devices physically secure.
- Use devices in accordance with school procedures.
- Ensure devices receive updates when required.
- Report loss, theft or damage immediately.

Staff must not:

- Remove security settings.
- Install unauthorised software.
- Allow unauthorised individuals to use school devices.
- Make unauthorised changes to system configurations.

7. Home and Remote Working

When accessing school systems away from school, staff must:

- Use secure, password-protected Wi-Fi.
- Lock devices when unattended.
- Ensure confidential information cannot be viewed by others.
- Keep paper documents secure.
- Dispose of confidential waste appropriately.
- Follow all school security and data protection procedures.
- School devices must not be used by family members or other unauthorised individuals.

8. Personal Devices (BYOD)

Where personal devices are used to access approved school systems:

Staff must:

- Use strong passwords, PINs or biometric protection.
- Keep operating systems updated.
- Enable Multi-Factor Authentication where available.
- Report loss or theft immediately if school data may be affected.

Staff must not:

DRAFT

- Store confidential school information permanently on personal devices.
- Use personal devices for photographing or recording pupils.
- Circumvent school security measures.

9. Use of the Internet

Internet access is provided to support teaching, learning and school business.

Staff must:

- Use internet resources appropriately and legally.
- Respect copyright and licensing requirements.
- Evaluate online information critically before use.
- Report inappropriate content accessed accidentally.

Staff must not:

- Access illegal, offensive or inappropriate material.
- Download unauthorised software.
- Circumvent filtering systems.
- Engage in hacking or similar activity.
- Access data or systems for which they do not have authorisation.
- The Computer Misuse Act applies to all users of school ICT systems.

10. Artificial Intelligence (AI)

The school recognises the potential benefits of Artificial Intelligence (AI) when used responsibly.

Staff may:

- Use school-approved AI tools to support planning, administration and professional tasks.
- Use AI to assist with drafting content, provided all outputs are reviewed and amended as necessary.

Staff must not:

- Input personal pupil information.
- Input safeguarding information.
- Input medical information.
- Input confidential staff information.
- Input data that could identify pupils, families or colleagues.

Staff must:

- Verify the accuracy of AI-generated content before use.
- Exercise professional judgement at all times.
- Ensure AI use complies with safeguarding and data protection requirements.
- Inform senior leaders of any concerns regarding AI use.
- AI tools must never replace professional decision-making, particularly in safeguarding matters.

11. Email Use

School email accounts are provided for school business.

Staff must:

- Use professional language in all communications.
- Ensure emails are accurate before sending.
- Use secure methods when sharing sensitive information.
- Save important communication in accordance with school procedures.
- Exercise caution when opening links and attachments.

DRAFT

Staff must not:

- Impersonate another person.
- Send offensive, discriminatory or inappropriate content.
- Share confidential information without authorisation.
- Use personal email accounts for school business.

The school reserves the right to access emails where necessary for operational, safeguarding, legal or investigative purposes.

12. Social Media

Staff are expected to maintain the highest professional standards on social media.

Staff must:

- Ensure personal use does not affect professional responsibilities.
- Use privacy settings appropriately.
- Consider how online activity may reflect on the school.

Staff must not:

- Discuss pupils, families or colleagues online.
- Share confidential information.
- Publish content that may damage the reputation of the school.
- Engage in online conduct that could constitute bullying, discrimination or harassment.
- Communicate with pupils via personal social media accounts.
- Official school social media accounts may only be used with authorisation from senior leaders.

13. Photography, Video and Audio Recording

Staff must:

- Use only school-approved devices.
- Follow parental consent arrangements.
- Store images securely.
- Use recordings only for authorised school purposes.

Staff must not:

- Use personal devices to photograph or record pupils.
- Share images through personal accounts or applications.
- Store pupil images on unauthorised devices or locations.

14. Data Protection and Confidentiality

All information relating to pupils, staff and families must be treated as confidential.

Staff must:

- Comply with UK GDPR and the Data Protection Act 2018.
- Access only information required for their role.
- Store personal data securely.
- Share information only where authorised and necessary.
- Follow school retention and disposal procedures.

Staff must not:

- Access records without a legitimate reason.
- Disclose confidential information inappropriately.
- Discuss sensitive information in public places.

DRAFT

- Leave confidential information unattended.

15. Cyber Security

Staff must:

- Use strong passwords.
- Keep passwords confidential.
- Enable Multi-Factor Authentication where available.
- Report suspected phishing emails immediately.
- Lock devices when leaving them unattended.
- Report cyber security concerns promptly.

Staff must not:

- Share passwords.
- Approve authentication requests they have not initiated.
- Open suspicious attachments knowingly.
- Ignore cyber security warnings.

16. Data Breach Reporting

Any actual or suspected breach involving personal information must be reported immediately to:

The Headteacher.(SA)

The Data Protection Officer. (SL)

Or another designated senior leader. (MH)

Prompt reporting allows the school to meet its legal reporting obligations and minimise risks to affected individuals.

17. Monitoring

The school reserves the right to monitor, access, review and retain information stored on or transmitted through school systems where this is necessary for:

- Safeguarding.
- Network security.
- Investigations.
- Compliance with legal requirements.
- Prevention and detection of misconduct.
- Business continuity and operational purposes.

Staff should have no expectation of privacy when using school-owned ICT systems.

18. Reporting Concerns

Staff must immediately report:

- Safeguarding concerns.
- Data breaches.
- Cyber security incidents.
- Loss or theft of devices.
- Inappropriate online content.
- Suspected misuse of ICT systems.

19. Breaches of this Policy

DRAFT

- Failure to comply with this policy may result in:
- Informal management action.
- Additional training.
- Removal of ICT access.
- Disciplinary action.
- Referral to external agencies where appropriate.
- Referral to professional regulatory bodies.
- Referral to the Local Authority, DBS, ICO or Police where necessary.
- Serious breaches may constitute gross misconduct.

20. Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Online Safety Policy
- Data Protection Policy
- Behaviour Policy
- Whistleblowing Policy

DRAFT