



WREN'S NEST PRIMARY SCHOOL

Key Policy 2026-2027

Home Working Policy

September 2026

Document to be read in conjunction with other key school policies

Home Working Policy – Wren’s Nest Primary School

1. Purpose

This policy sets out the expectations, responsibilities, and safeguards required for staff undertaking approved home working. It ensures remote working supports flexibility while maintaining productivity, safeguarding, confidentiality, and compliance with statutory requirements including the Data Protection Act 2018 and UK GDPR.

This policy applies to all staff who work from home on a full-time, part-time, occasional, or ad-hoc basis.

2. Principles of Home Working

Home working must uphold the same professional standards as on-site working. Key principles include:

- Protecting personal data in line with Article 5(1)(f) UK GDPR: ensuring integrity and confidentiality.
- Preventing unauthorised access, accidental loss, destruction, or damage to information.
- Maintaining safeguarding standards at all times.
- Ensuring staff remain contactable, productive, and compliant with school policies.
- Using school-approved systems, devices, and communication channels.
- Recognising that information security is more important than equipment security.

3. Approval and Eligibility

Home working must be approved by the Headteacher or line manager. Approval considers:

- Role suitability
- Operational needs
- Safeguarding implications
- Data protection requirements
- Health and safety considerations

Staff must sign the Home Working Agreement (Appendix A) before commencing home working.

4. Status of the Working Day

- A home-working day is treated as a normal contracted working day.
- Staff must be available and working during usual hours unless agreed otherwise.
- Duties, deadlines, and responsibilities remain unchanged.
- Staff must attend virtual meetings and respond to communication promptly.

5. Attendance, Communication and Availability

Staff must:

- Be reachable via email, telephone, or agreed platforms.
- Respond within reasonable timeframes.
- Manage short periods of unavailability appropriately.
- Report technical issues immediately.

6. Safeguarding and Professional Conduct

Staff must:

- Maintain professional boundaries when communicating with pupils and families.
- Use only school-approved platforms for communication.
- Ensure conversations cannot be overheard by household members.
- Ensure screens cannot be viewed by unauthorised individuals.
- Report safeguarding concerns immediately in line with statutory guidance.

7. Data Protection, Confidentiality and Information Security

7.1 Personal Data Handling

Staff must:

- Access only the information necessary for their role and avoid removing full pupil files unless essential.
- Keep a record of any paper documents taken home and returned.
- Store paper documents securely in locked cases or cabinets.
- Never leave papers or devices in vehicles, especially overnight.
- Keep paper records separate from electronic devices to reduce theft impact.

7.2 Electronic Security

- Use school devices wherever possible.
- Personal devices must **not** store or process school data.
- Devices must be password-protected and locked when unattended.
- Home networks must be secure; multi-factor authentication should be used where available.
- Staff must remain vigilant to phishing attempts and verify suspicious messages.

7.3 Email

- Only school email accounts may be used for school business (not personal or any third-party accounts).
- Staff must ensure family members cannot access school email accounts on shared devices.

7.4 Video Conferencing

Staff must:

- Use school-approved platforms (e.g., Microsoft Teams).
- Check privacy and security settings before meetings.
- Restrict access using passwords or waiting rooms.
- Ensure surroundings are confidential and free from reflective surfaces.
- Keep software and browsers up to date.
- Avoid sharing personal or sensitive data unless essential.

8. Working Environment

Staff must ensure:

- A confidential workspace free from household access.
- Reliable internet access.
- Safe workstation setup (posture, screen height, lighting).
- Equipment is kept out of sight when not in use.
- Conversations and screen content cannot be overheard or viewed.

9. Health, Safety and Wellbeing

- Staff are responsible for maintaining a safe home working environment.
- Regular breaks should be taken in line with display screen equipment guidance.
- Any health and safety concerns must be reported.
- The school may request completion of a home-working risk assessment.

10. Use of School Equipment

- School equipment must be used for work purposes only.
- Equipment must be stored securely and returned when requested.
- Loss, theft, or damage must be reported immediately.
- Equipment must not be left in vehicles or visible to visitors.

11. Transit and Storage of Information

Staff must:

- Transport documents securely and go directly home when carrying sensitive information.
- Remove documents from vehicles immediately.
- Avoid shops or stops while transporting confidential material.

12. Disposal of Paper, Media and Equipment

- Paper documents containing personal data must be cross-cut shredded.
- Equipment must be disposed of through approved school processes.
- Personal data must never be placed in household waste.

13. Personal Responsibility and Accountability

Staff must:

- Comply with all school policies while working from home.
- Complete required Information Governance training.
- Understand that breaches may result in disciplinary action.
- Recognise that individuals can face civil action under UK GDPR for data loss.

14. Consequences of Data Breaches

Any loss, theft, or unauthorised disclosure of personal data must be reported immediately to the Headteacher or Chair of Governors.

Consequences may include:

- Safeguarding implications
- ICO investigation
- Reputational damage
- Disciplinary action

If the breach involves a looked-after child, the Designated Safeguarding Lead must be notified immediately.

15. Review, Monitoring and Compliance

- Home-working arrangements may be reviewed at any time.
- The school may withdraw home-working arrangements where necessary.
- This policy will be reviewed annually or sooner if required.

Staff must ensure they have read and understood the following school policies, which apply fully when working from home and should be followed in conjunction with the Home Working Agreement:

- Data Protection Policy
- Information Security Policy
- Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Retention Policy
- Health and Safety Policy
- Staff Code of Conduct